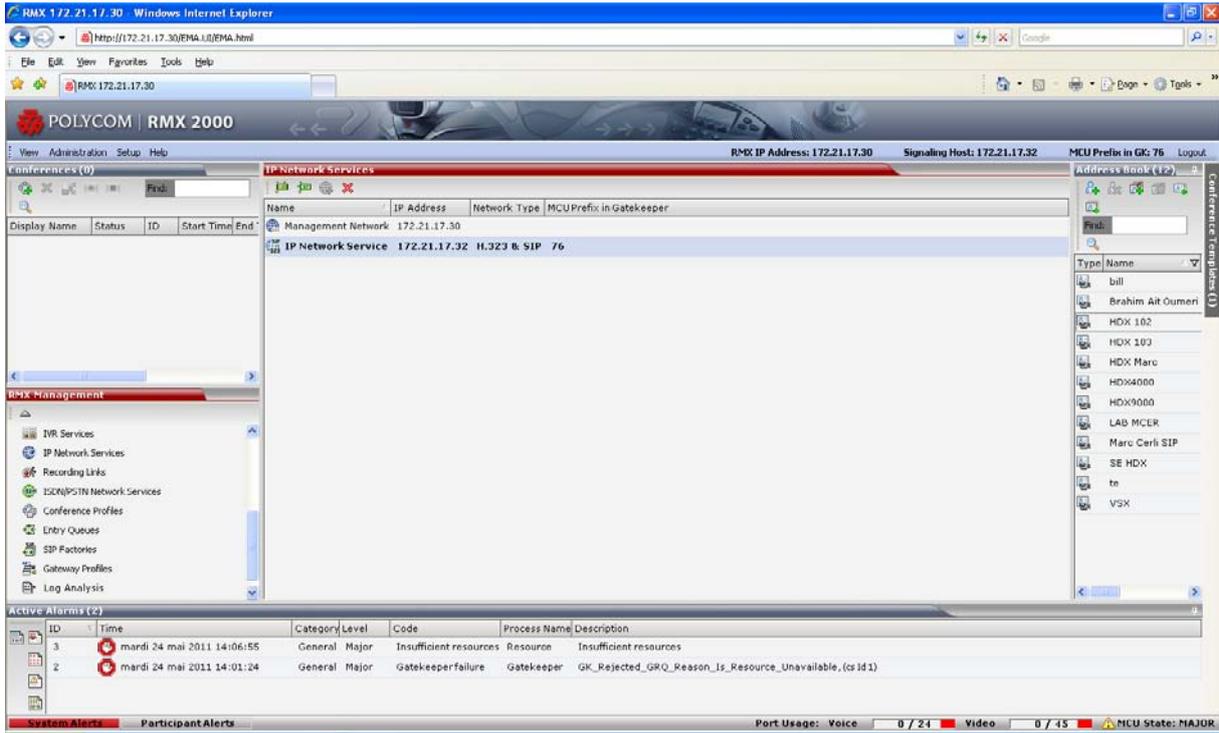


Steps procedure for integrating RMX solution into Lync environment

Document prepared by Brahim AIT OUMERI - MS UC Solutions Architect - Polycom EMEA

E-mail: brahim.aitoumeri@polycom.com

Login on the RMX2000 :



Go in the Management Network Properties

The screenshot shows the 'Management Network Properties' dialog box. The left sidebar contains a tree view with the following items: IP, Routers, DNS (selected), and LAN Ports. The main content area is divided into several sections:

- Network Service Name:** A text box containing 'Management Network'.
- MCU Host Name:** A text box containing 'rmx2000s1'.
- DNS:** A dropdown menu set to 'Specify'.
- Register Host Names Automatically to DNS Servers:** An unchecked checkbox.
- Local Domain Name:** A text box containing 'polycomlive.com'.
- DNS Servers Addresses:** Three text boxes for Primary, Secondary, and Tertiary servers, containing '172.21.17.4', '0.0.0.0', and '0.0.0.0' respectively.

At the bottom right, there are 'OK' and 'Cancel' buttons.

Enter the following related information :

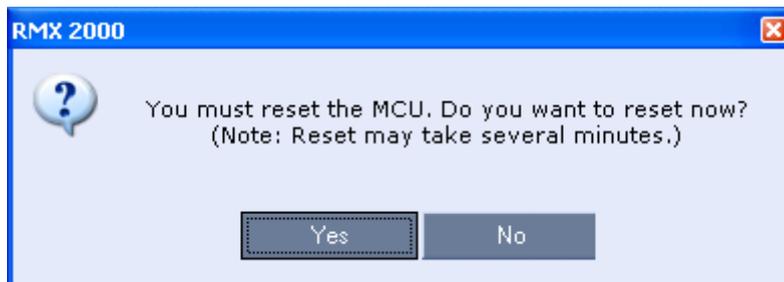
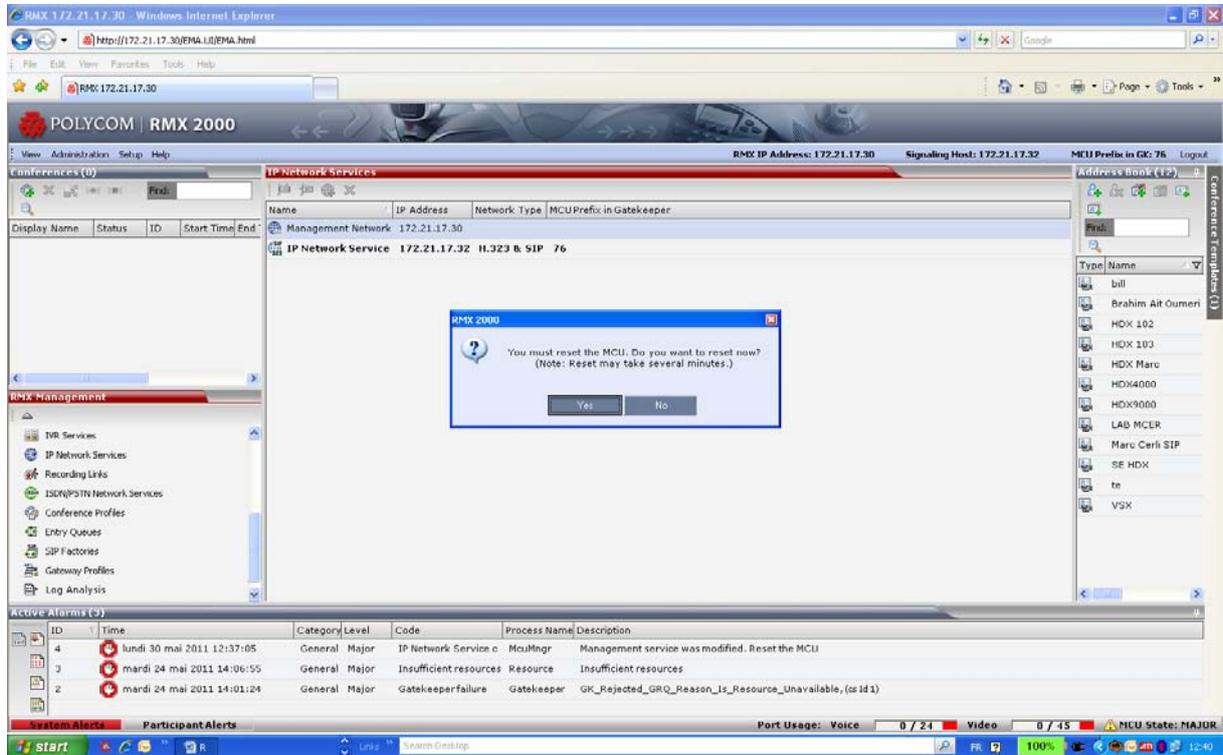
MCU Host Name : **rmx2000s1** (enter here the hostname of the RMX)

DNS: **Specify** (enter here "Specify")

Local Domain Name: **polycomlive.com** (enter here the domain name where Lync is hosted; for example, if FQDN of Lync is lync01.domain.com, then enter "domain.com")

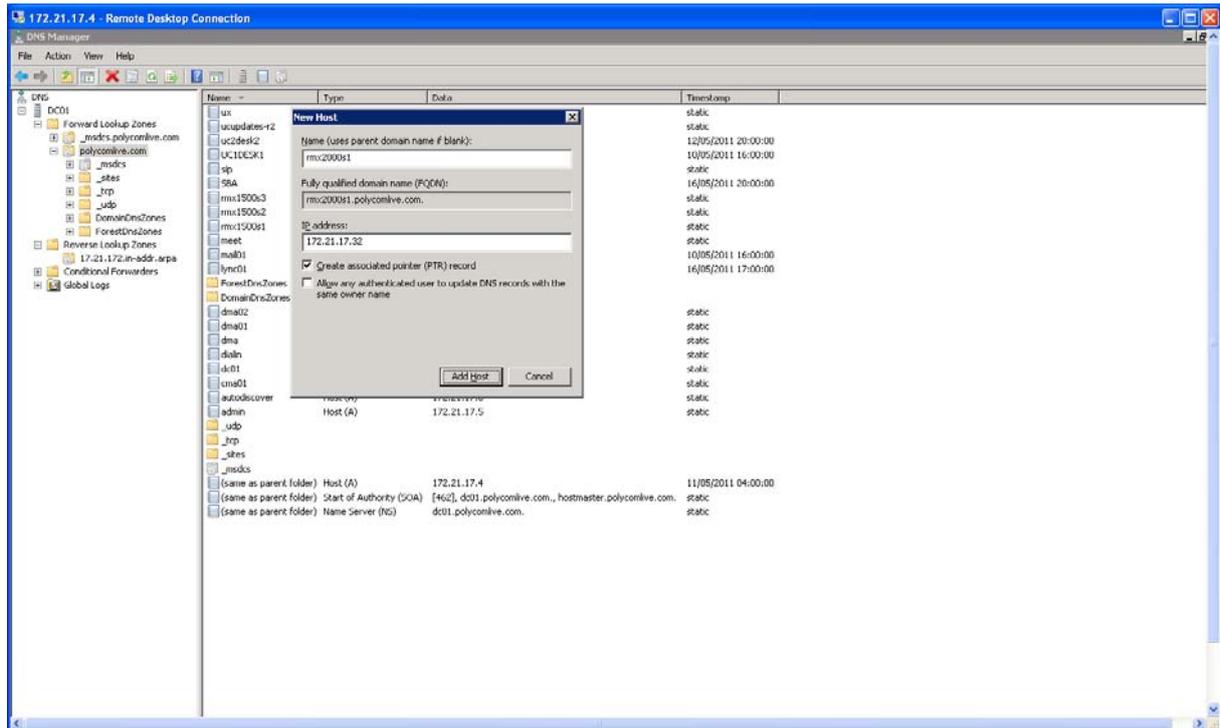
Primary Server: **172.21.17.4** (enter here the IP address of the DNS server RMX)

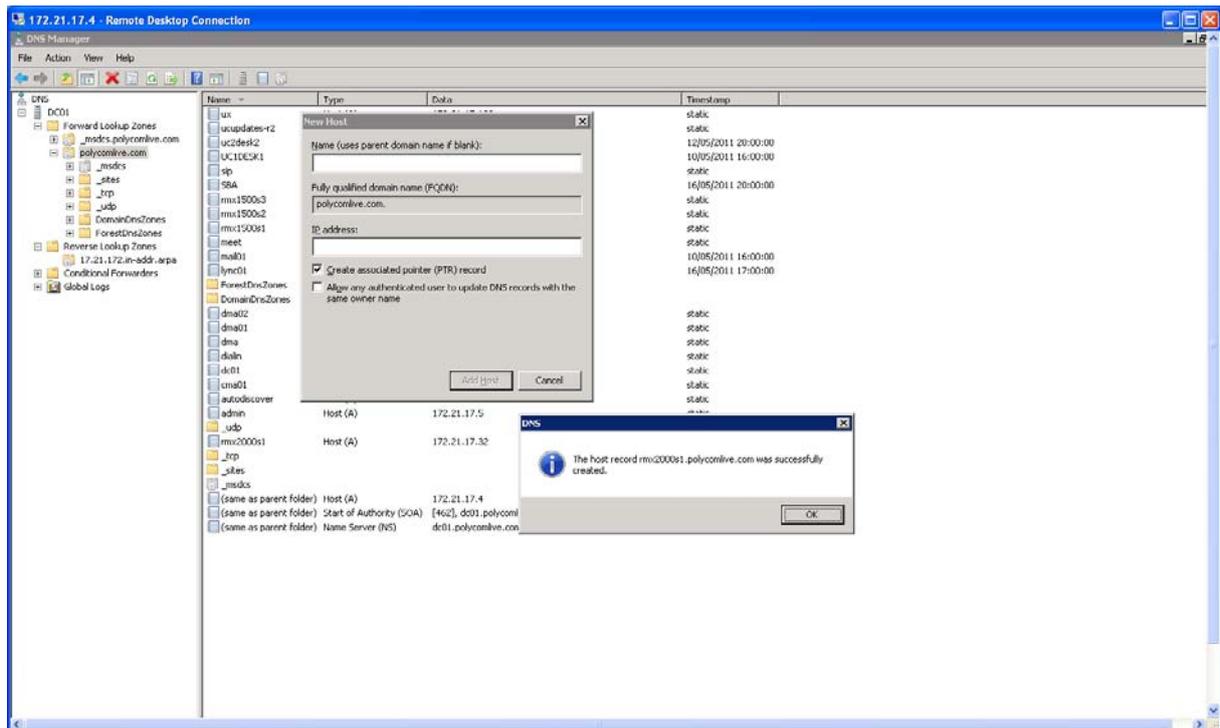
After this reboot the RMX server:



Then, login on the DNS server parent and Add the RMX FQDN in DNS pointing to the Signalling IP address of the RMX.

In the example of the RMX shown previously, the Signalling IP address is: 172.21.17.32

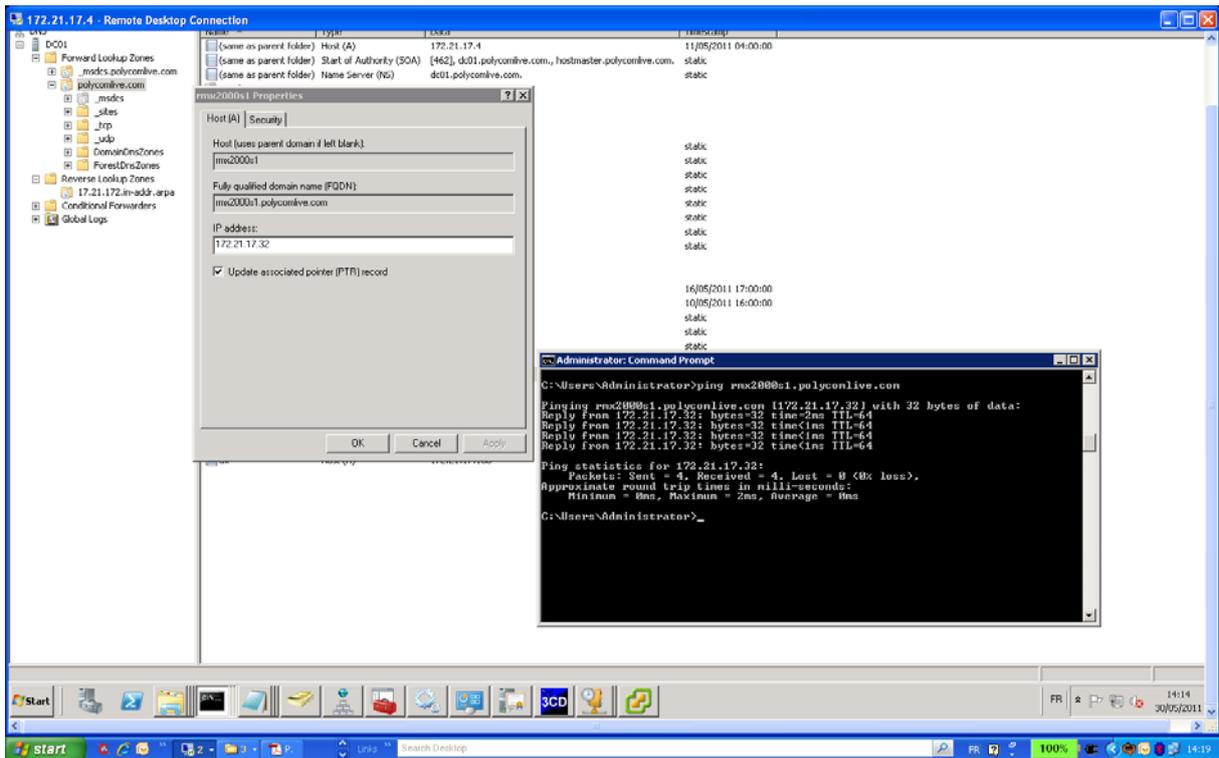




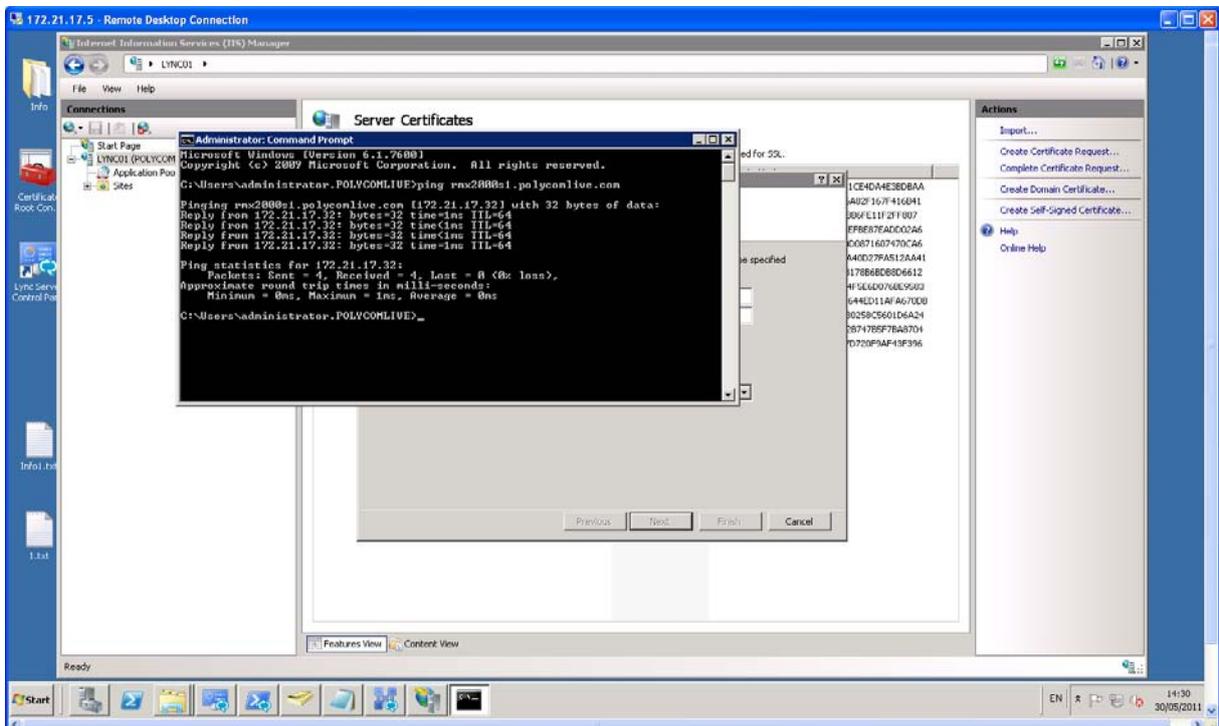
Once the DNS RMX Signalling IP record entry is added, run the nslookup command on the Lync server to check that the RMX FQDN is resolved by the Lync server.

You can also check if you can ping the FQDN of the RMX from the DNS server and then from Lync server as shown below.

Ping from DNS server:



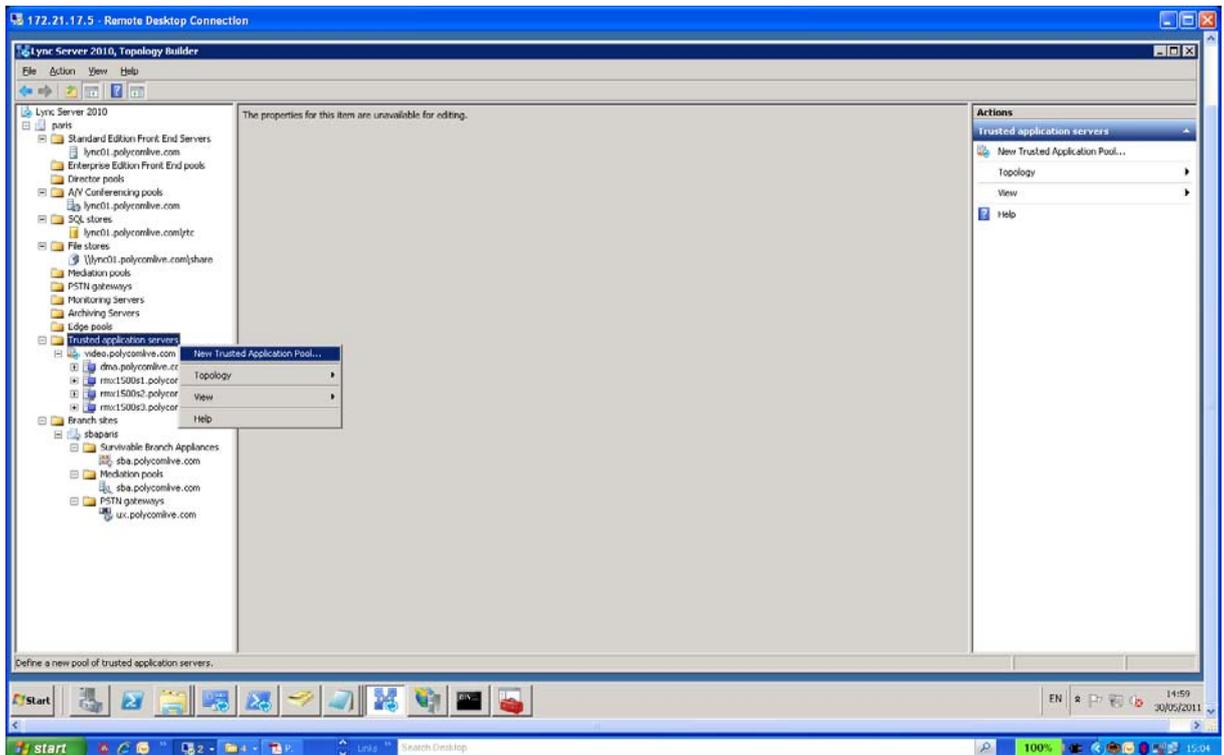
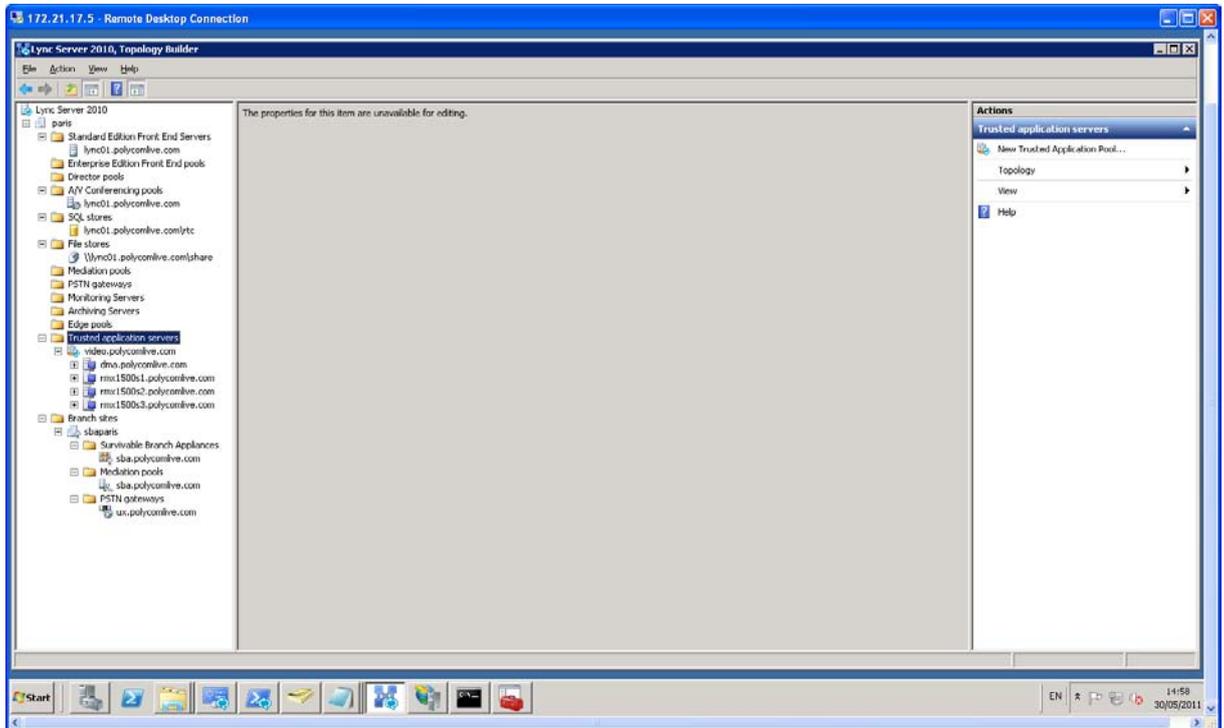
Ping from Lync:



Then, login on the Lync server and run the following steps.

Set the Routing for the Polycom RMX System

1- Use Lync Topology Builder to define your trusted application pool



Enter for example the following trusted entry name:

rmx2kvideo.polycomlive.com

This entry will be used to call the RMX meeting rooms from Lync client.

For example, to call meeting room 1001 from Lync client, you will need to call the following SIP URI from Lync client:

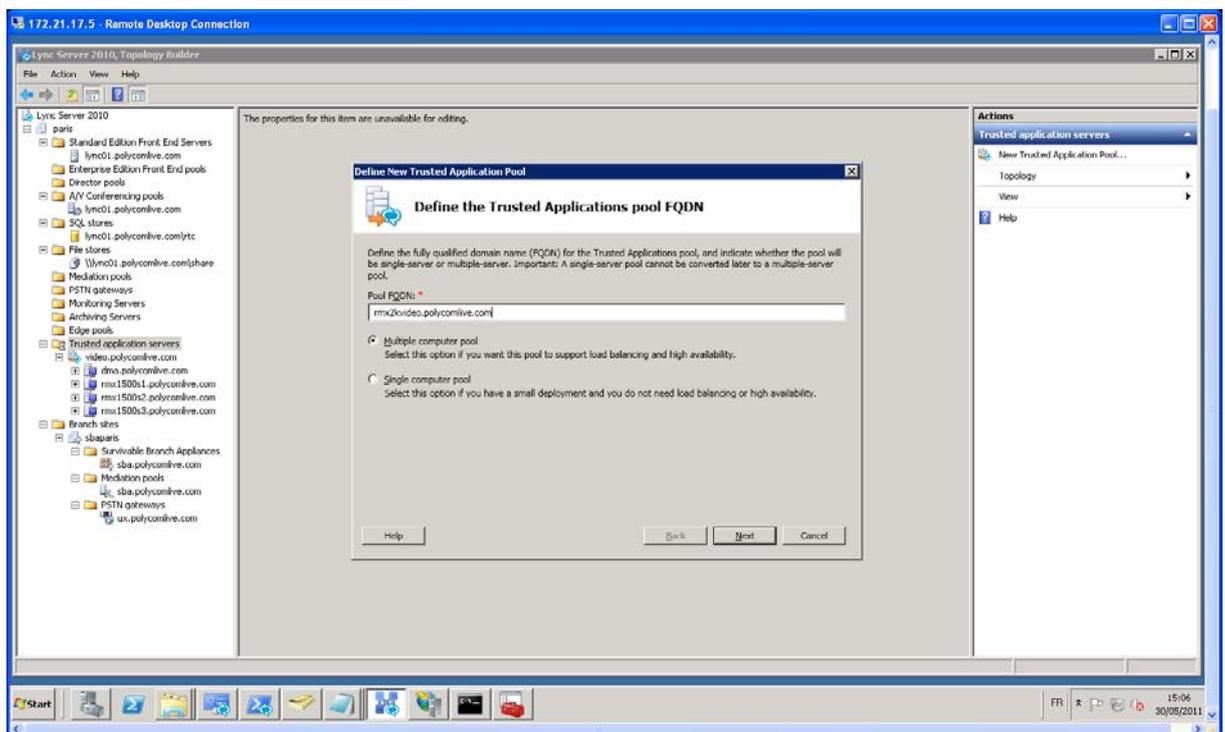
1001@rmx2kvideo.polycomlive.com

In your case, you can enter:

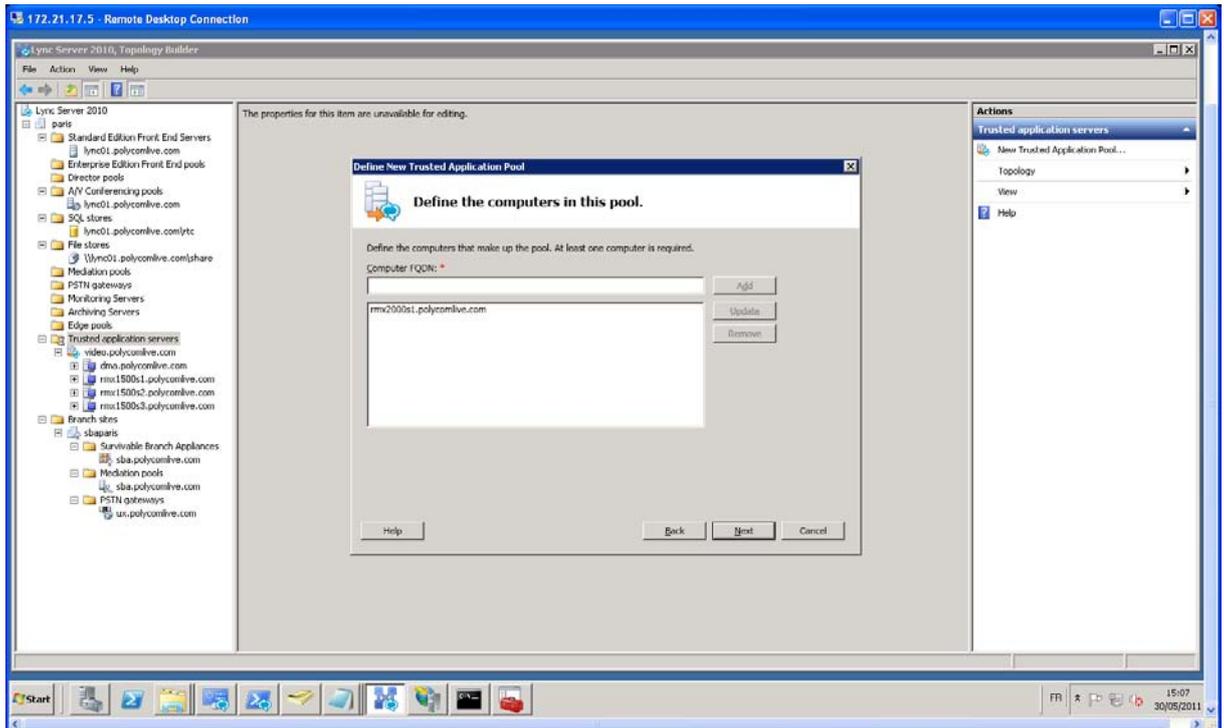
rmx2kvideo.domain.com (in case your domain name is "domain.com").

In this case, you will call 1001 meeting room from Lync client using the following SIP URI:

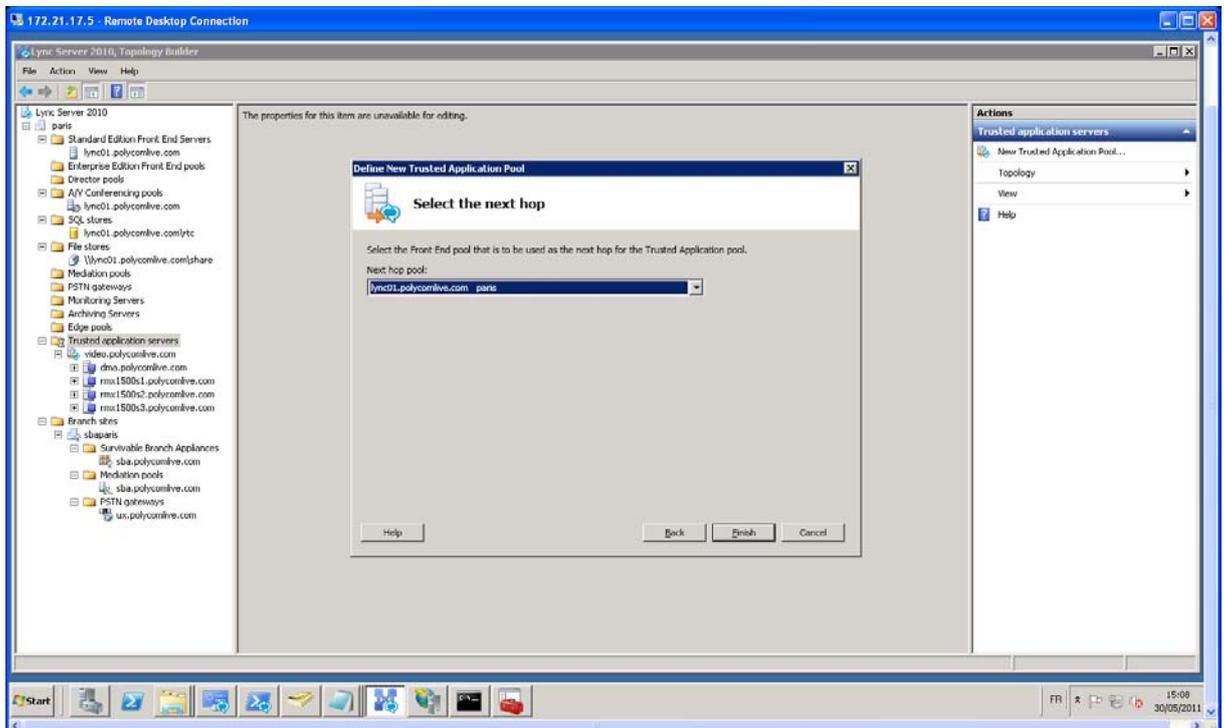
1001@rmx2kvideo.domain.com



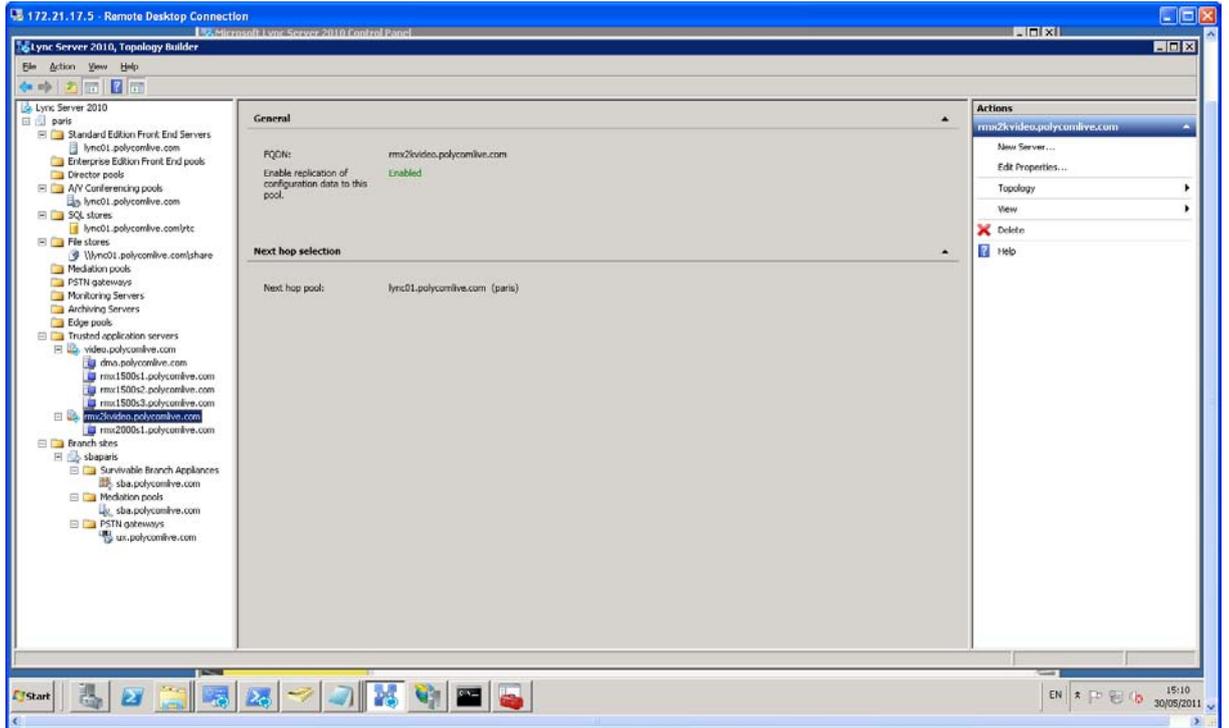
Then enter the FQDN of the RMX that you had defined in the DNS previously.
rmx2000s1.polycomlive.com (in this current example)



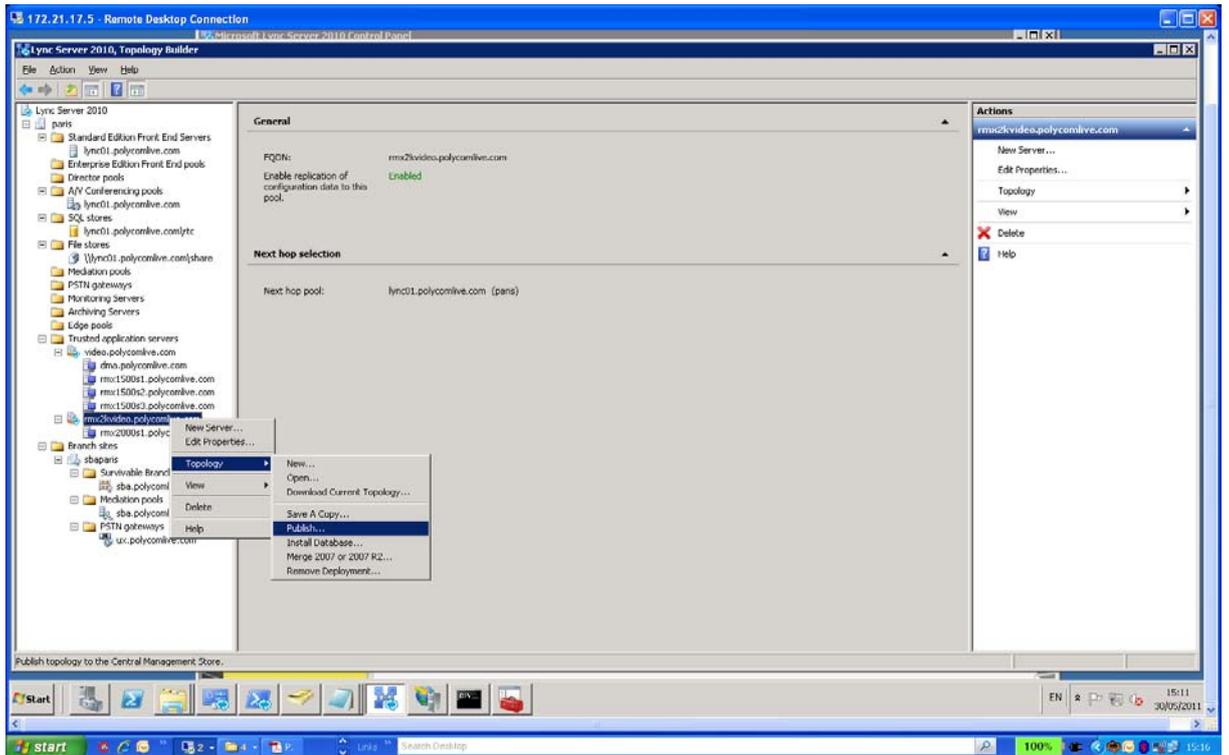
Select the Lync pool as shown below:



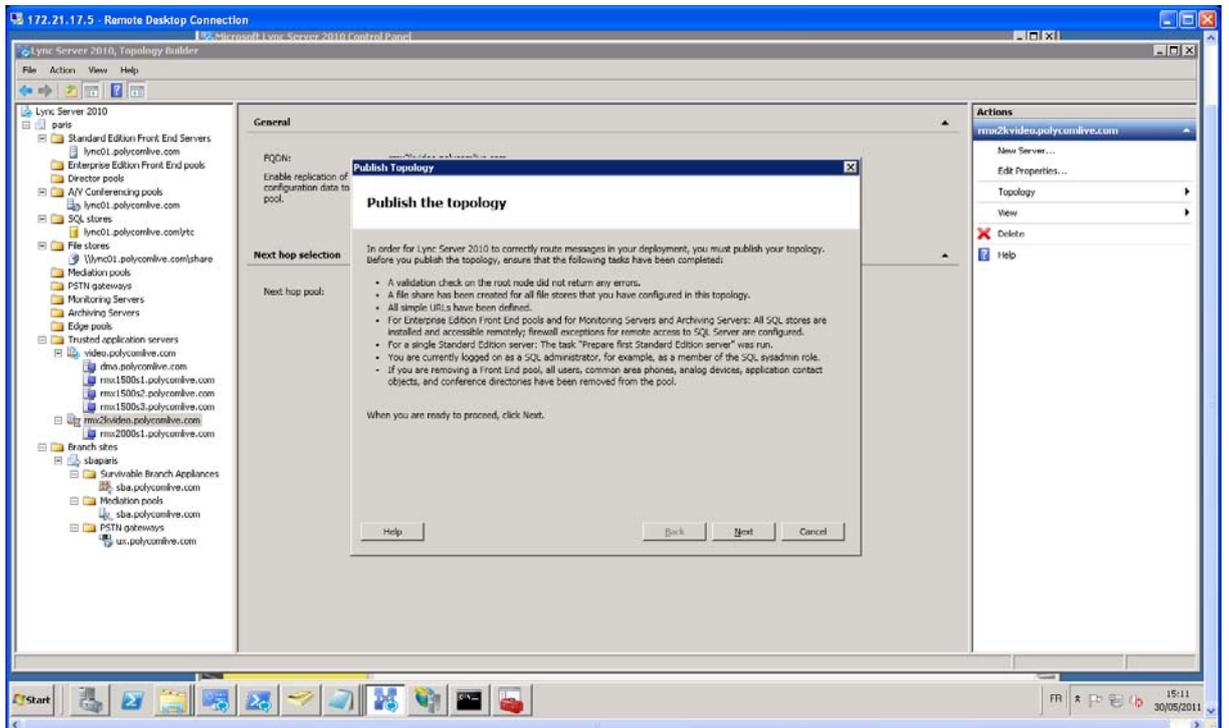
After this, you will see the new trusted entry as shown below:



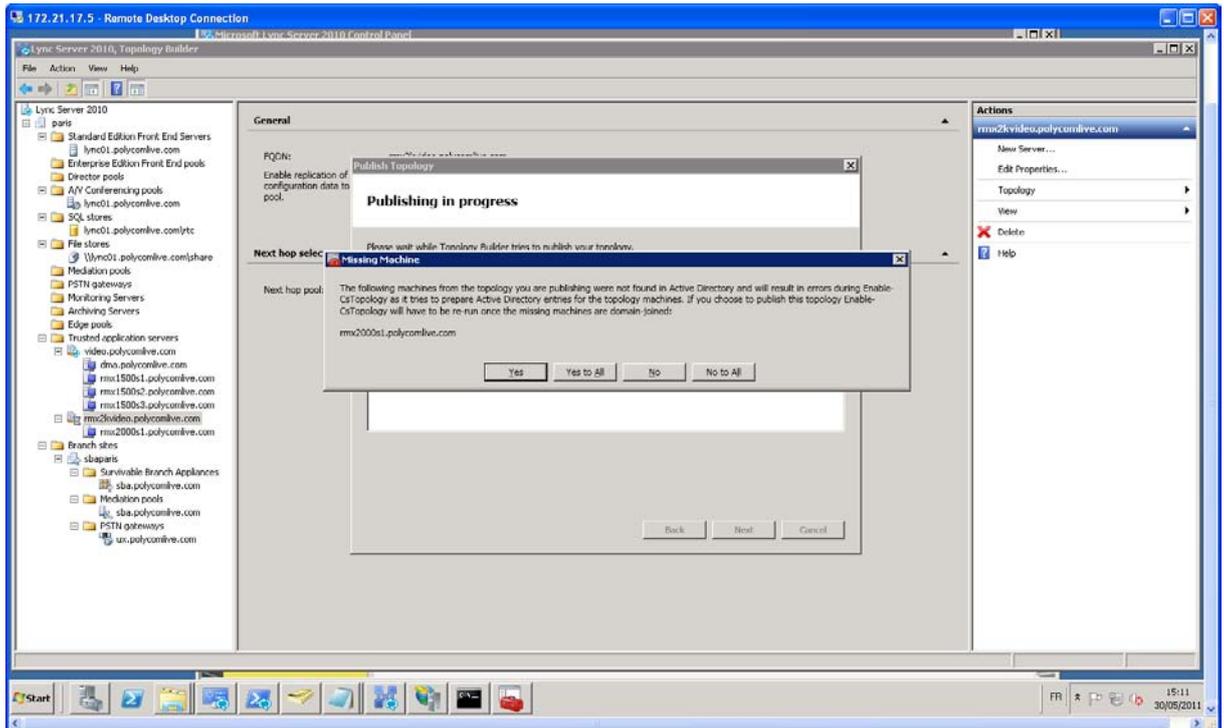
Then, right click on the new trusted entry and select “Topology”, then select “Publish” action, as shown below:



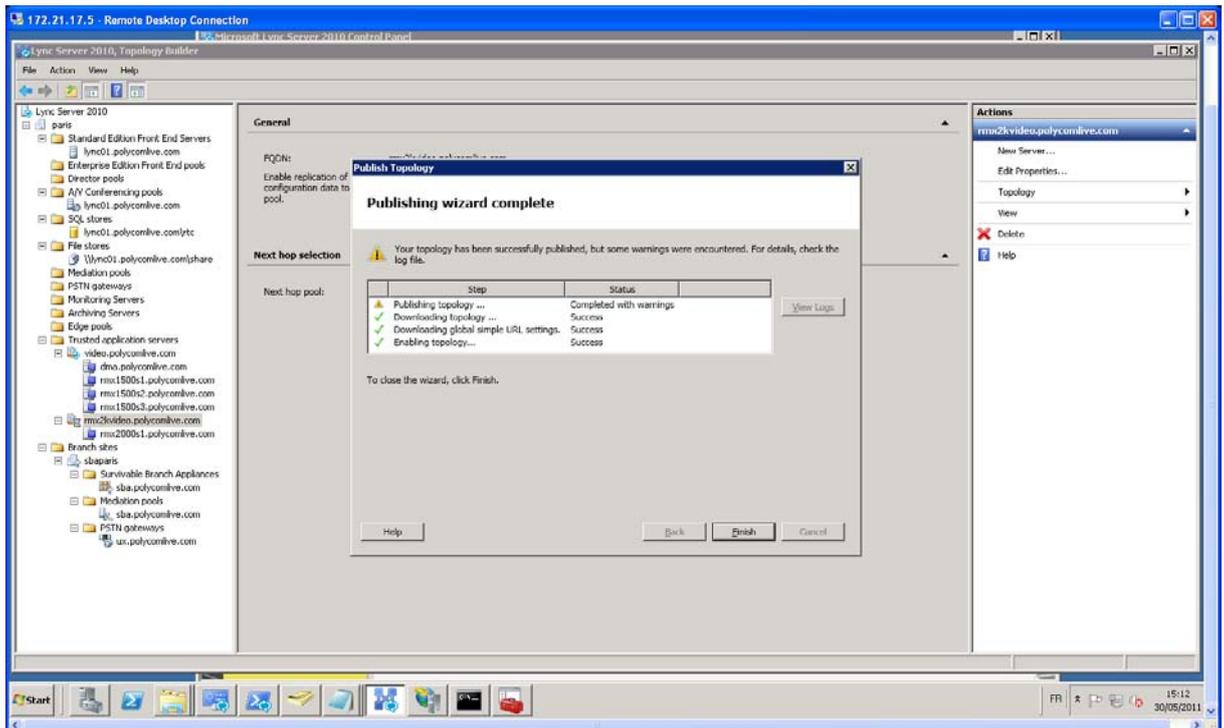
Select “Next”



Select "Yes to All"



Select "Finish"



Go in the “Lync Control Panel”, in “Topology” menu, in the “Status” section and verify that the RMX FQDN entry “rmx2000s1.polycomlive.com” is there in the list, as shown below: In this current example, the RMX FQDN entry “rmx2000s1.polycomlive.com”.

The screenshot shows the Microsoft Lync Server 2010 Control Panel. The left sidebar contains a navigation tree with categories like Home, Users, Topology, IM and Presence, Voice Routing, etc. The main area displays the 'Status' section of the 'Topology' menu. A table lists server details:

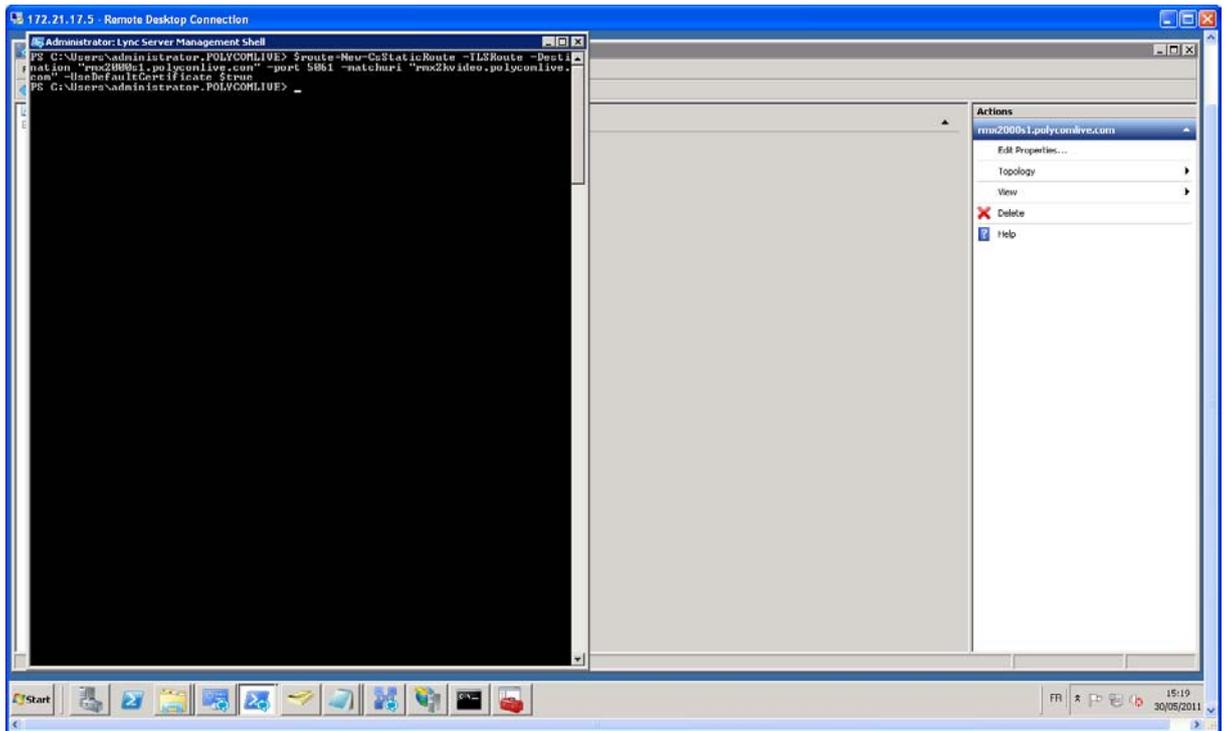
Computer	Pool	Site	Status	Replication
dms.polycomlive.com	video.polycomlive.com	paris	N/A	✗
lync01.polycomlive.com	Standard Edition	paris	✓	✓
rmx1500s1.polycomlive.com	video.polycomlive.com	paris	N/A	✗
rmx1500s2.polycomlive.com	video.polycomlive.com	paris	N/A	✗
rmx1500s3.polycomlive.com	video.polycomlive.com	paris	N/A	✗
rmx2000s1.polycomlive.com	rmx2video.polycomlive.com	paris	N/A	✗
sbs.polycomlive.com	sbs.polycomlive.com...	sbsparis	Retrieving	✗
ux.polycomlive.com	ux.polycomlive.com	sbsparis	N/A	N/A

2- Use Lync Powershell to set the Polycom RMX system as a trusted host with a static route

PS C:\Users\administrator.POLYCOMLIVE>

```
$route=New-CsStaticRoute -TLSSRoute -Destination "rmx2000s1.polycomlive.com" -port 5061 -matchuri "rmx2kvideo.polycomlive.com" -UseDefaultCertificate $true
```

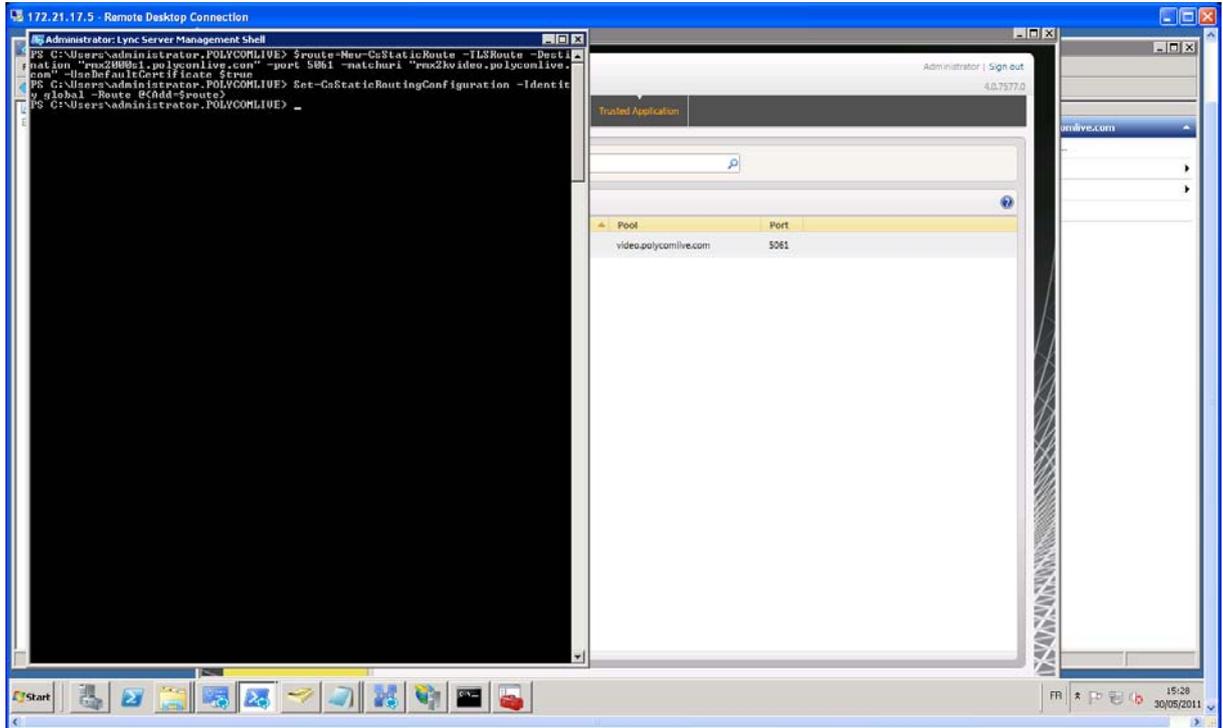
In this example "rmx2000s1.polycomlive.com" is the RMX FQDN and "rmx2kvideo.polycomlive.com" is the trusted entry defined previously.



After that, run the following command also to set the new route

PS C:\Users\administrator.POLYCOMLIVE>

Set-CsStaticRoutingConfiguration -Identity global -Route @{Add=\$route}



3- Use Lync Powershell to create the trusted application

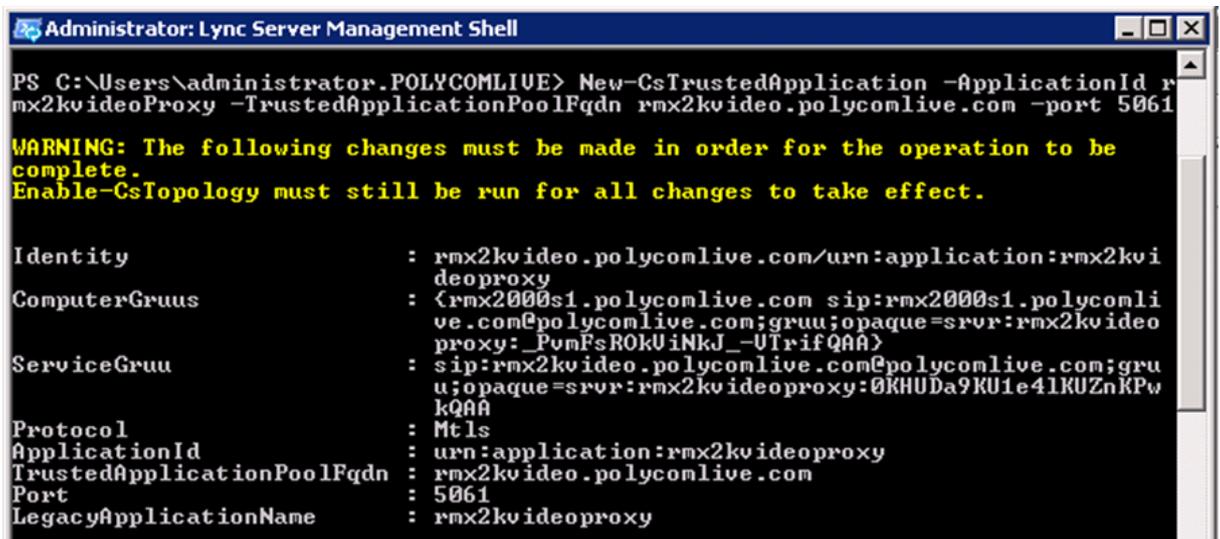
```
PS C:\Users\administrator.POLYCOMLIVE> New-CsTrustedApplication -ApplicationId rmx2kvideoProxy -TrustedApplicationPoolFqdn rmx2kvideo.polycomlive.com -port 5061
```

In this current example, **ApplicationId** is “**rmx2kvideoProxy**”.

In your example, you can enter exactly the same name. That will not have any negative impact on your setup.

In this current example, **TrustedApplicationPoolFqdn** is “**rmx2kvideo.polycomlive.com**”.

In your example, you have to enter the trusted entry you had created previously. In fact, it could be “**rmx2kvideo.domain.com**” if your domain name is “**domain.com**”.

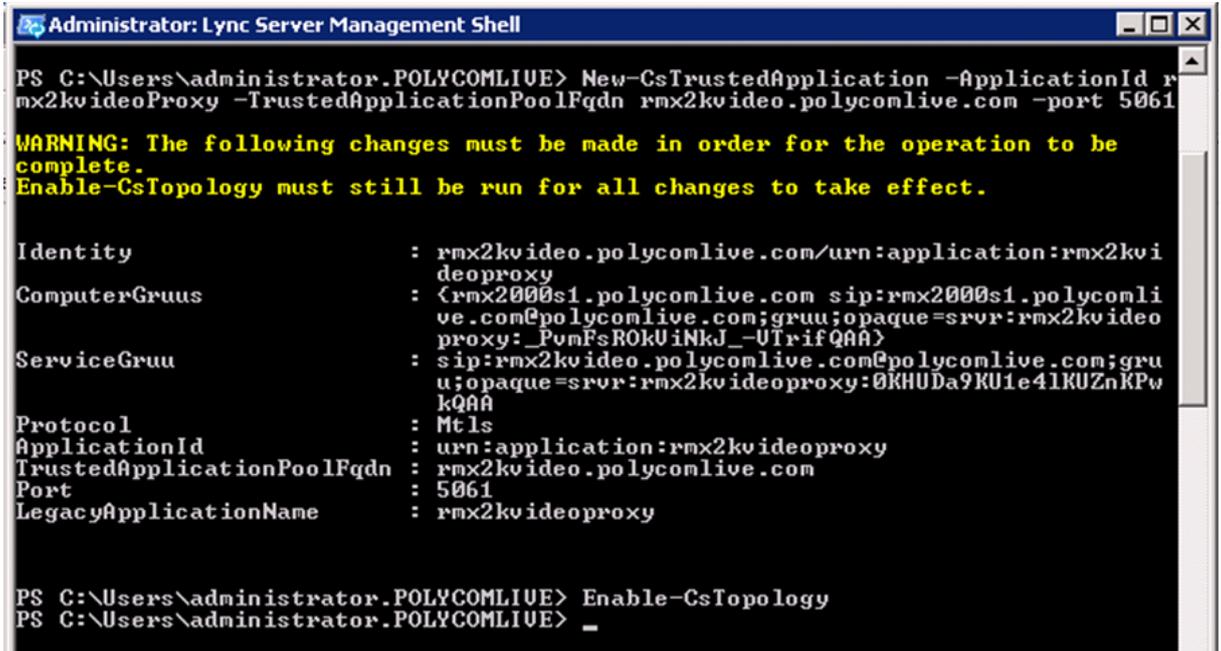


```
Administrator: Lync Server Management Shell
PS C:\Users\administrator.POLYCOMLIVE> New-CsTrustedApplication -ApplicationId rmx2kvideoProxy -TrustedApplicationPoolFqdn rmx2kvideo.polycomlive.com -port 5061
WARNING: The following changes must be made in order for the operation to be complete.
Enable-CsTopology must still be run for all changes to take effect.

Identity           : rmx2kvideo.polycomlive.com/urn:application:rmx2kvideoproxy
ComputerGrupos    : <rmx2000s1.polycomlive.com sip:rmx2000s1.polycomlive.com@polycomlive.com;gruu;opaque=srvr:rmx2kvideo
proxy:_PvmFsROkUiNkJ_-UTrifQAA>
ServiceGrupos     : sip:rmx2kvideo.polycomlive.com@polycomlive.com;gruu;opaque=srvr:rmx2kvideoproxy:0KHUda9KU1e41KUZnKPw
kQAA
Protocol          : Mtls
ApplicationId      : urn:application:rmx2kvideoproxy
TrustedApplicationPoolFqdn : rmx2kvideo.polycomlive.com
Port              : 5061
LegacyApplicationName : rmx2kvideoproxy
```

4- Use Lync Powershell to update the topology

PS C:\Users\administrator.POLYCOMLIVE> Enable-CsTopology



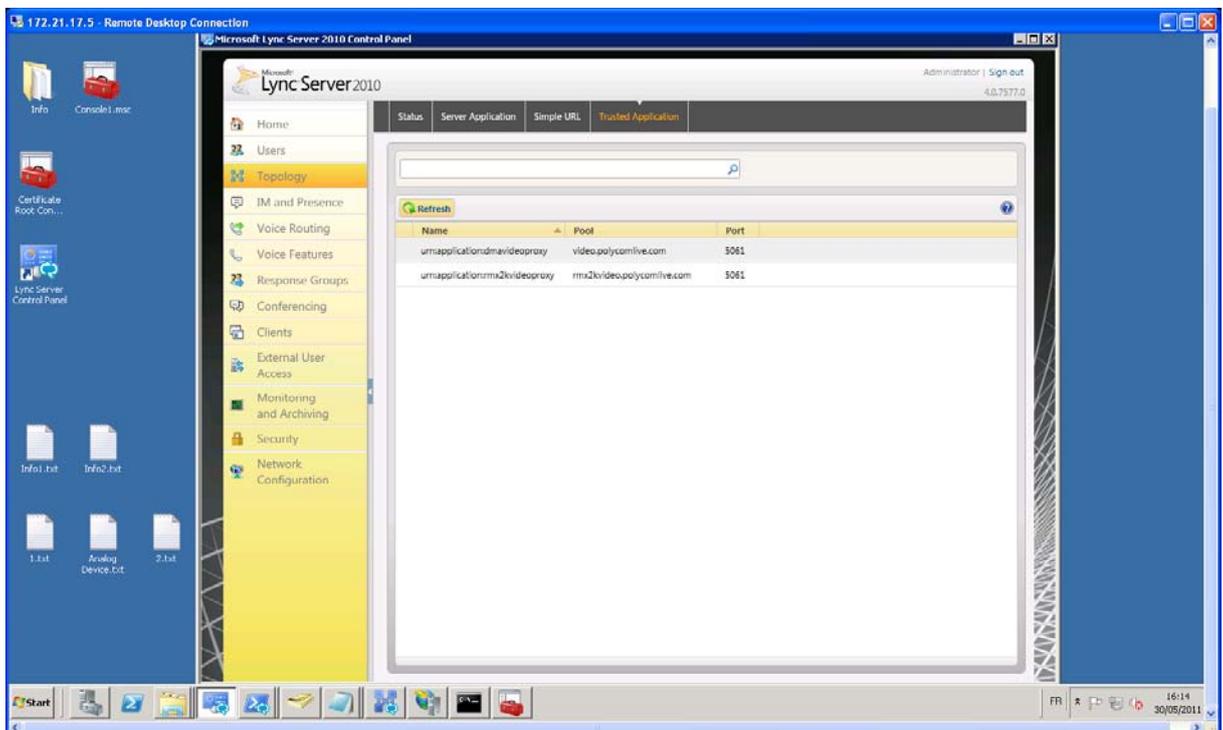
```
Administrator: Lync Server Management Shell
PS C:\Users\administrator.POLYCOMLIVE> New-CsTrustedApplication -ApplicationId rmx2kvideoProxy -TrustedApplicationPoolFqdn rmx2kvideo.polycomlive.com -port 5061
WARNING: The following changes must be made in order for the operation to be complete.
Enable-CsTopology must still be run for all changes to take effect.

Identity           : rmx2kvideo.polycomlive.com/urn:application:rmx2kvideoProxy
ComputerGrupos    : {rmx2000s1.polycomlive.com sip:rmx2000s1.polycomlive.com@polycomlive.com;gruu;opaque=srvr:rmx2kvideoProxy:_PumFsR0kUiNkJ_-UTrifQAA}
ServiceGrupos     : sip:rmx2kvideo.polycomlive.com@polycomlive.com;gruu;opaque=srvr:rmx2kvideoProxy:0KHUda9KU1e41KUZnkPwkQAA
Protocol          : Mtls
ApplicationId      : urn:application:rmx2kvideoProxy
TrustedApplicationPoolFqdn : rmx2kvideo.polycomlive.com
Port              : 5061
LegacyApplicationName : rmx2kvideoProxy

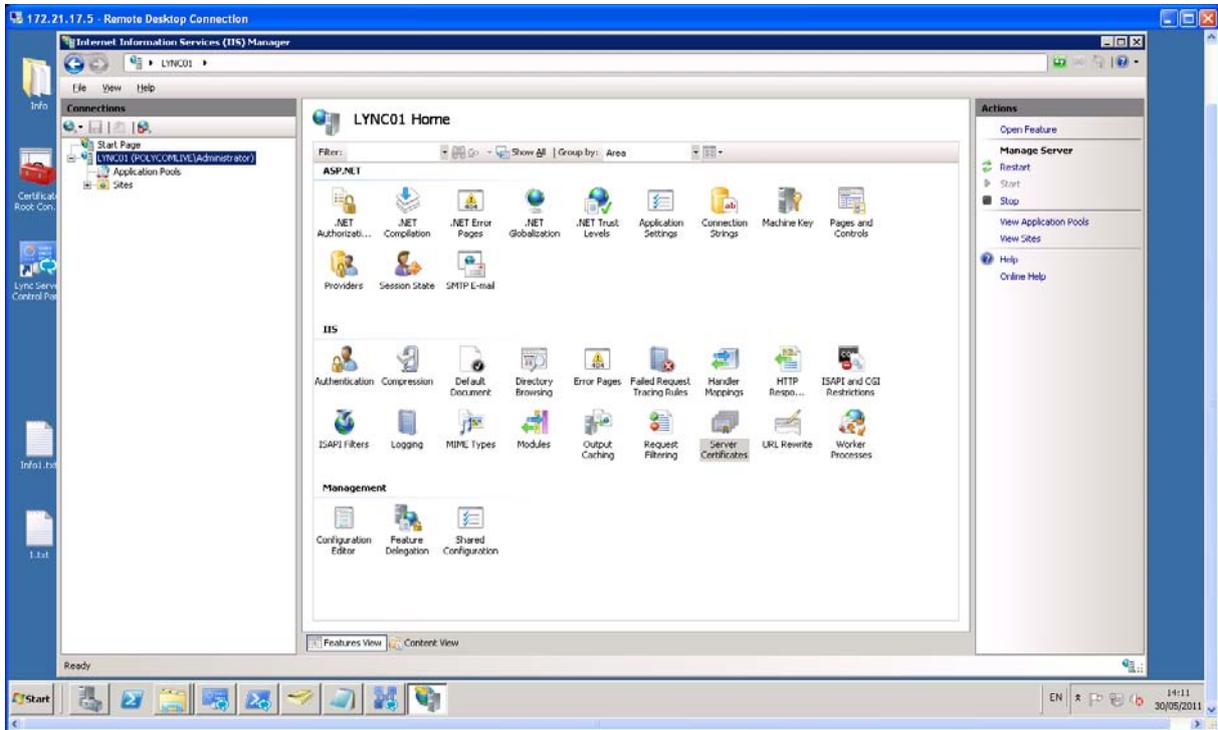
PS C:\Users\administrator.POLYCOMLIVE> Enable-CsTopology
PS C:\Users\administrator.POLYCOMLIVE> _
```

Go in the “Lync Control Panel”, in “Topology” menu, in the “Trusted Application” section and verify that the RMX Trusted entry “rmx2kvideo.polycomlive.com” is there in the list, as shown below:

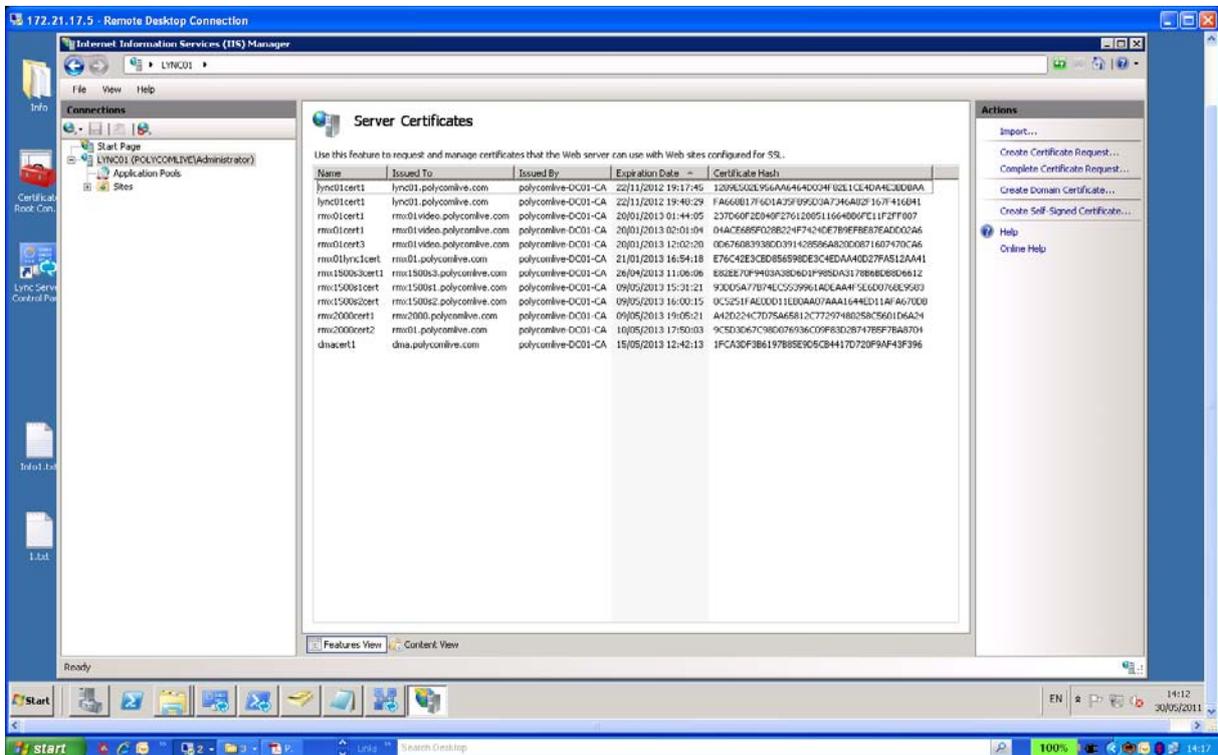
In this current example, the RMX Trusted entry is “rmx2kvideo.polycomlive.com”.



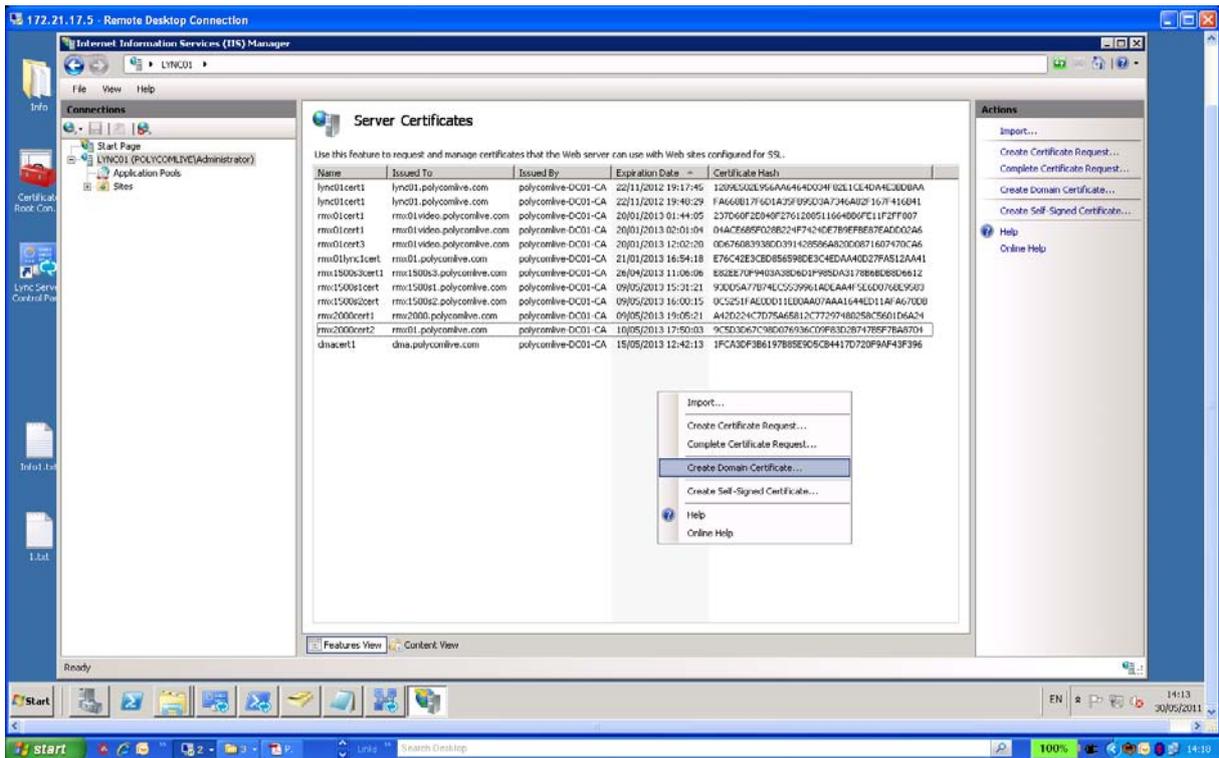
Login the Lync server and create a new certificate for RMX using the IIS Manager from the lync server, as shown below:



Double click on the "Server Certificate"

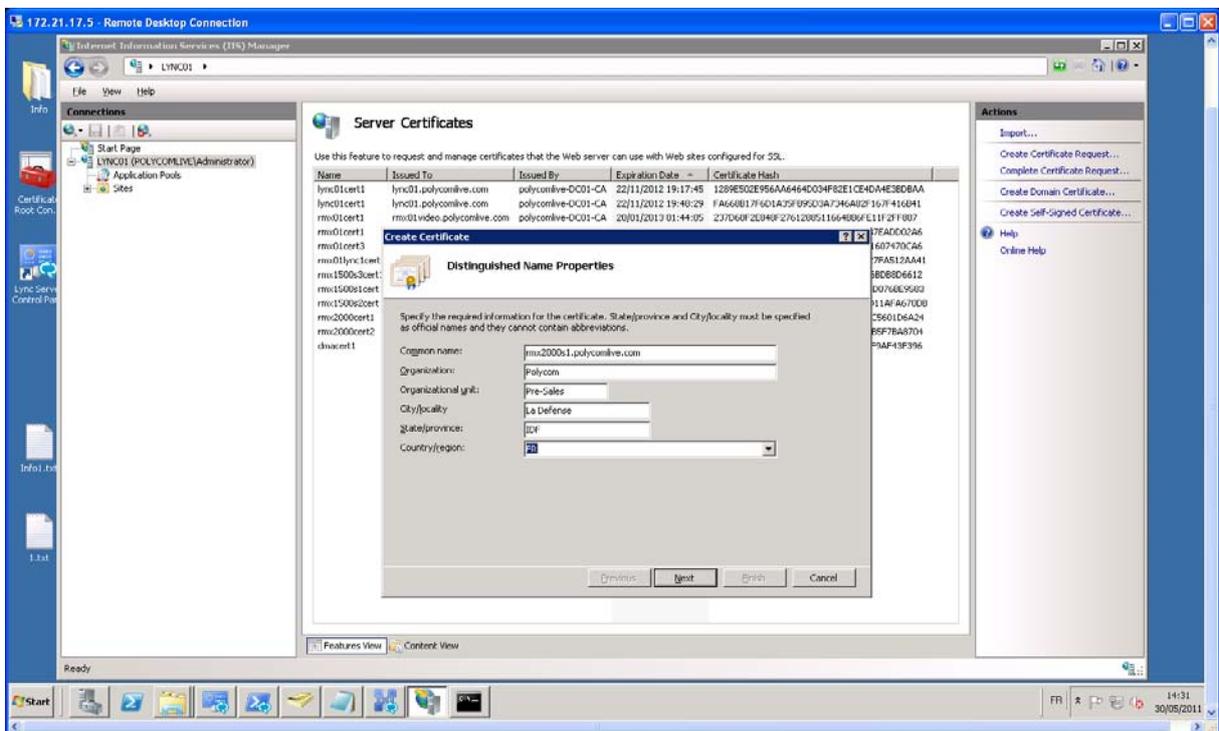


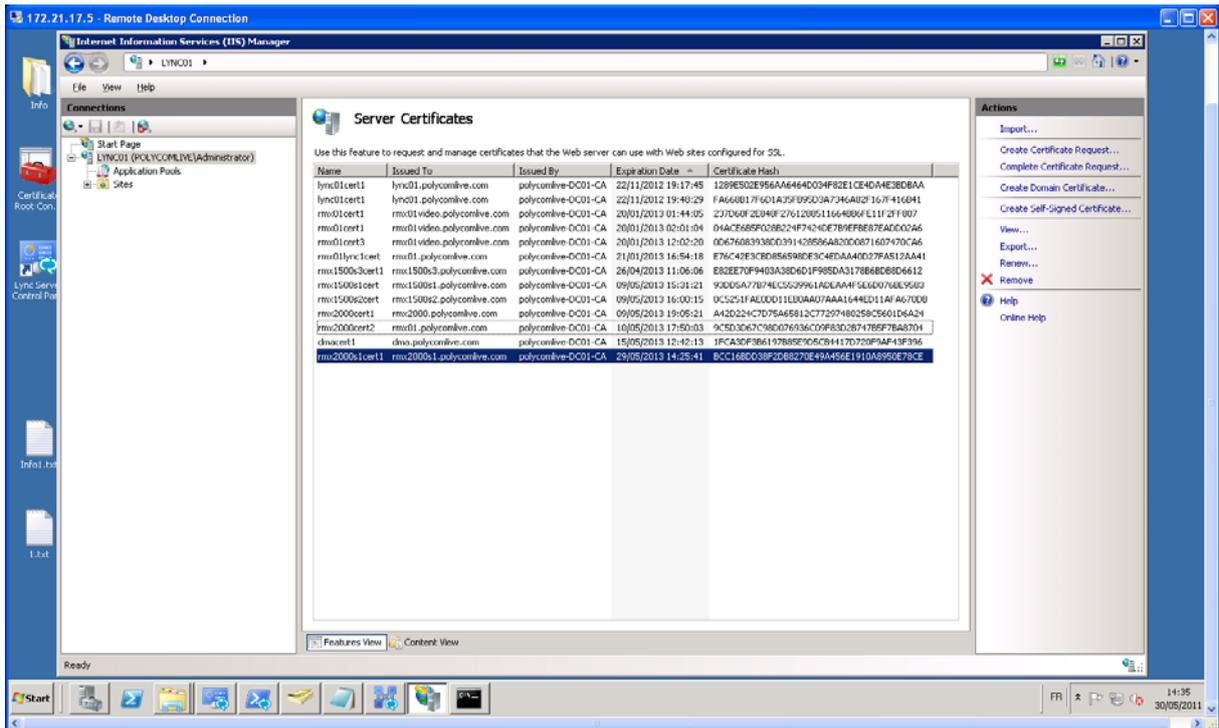
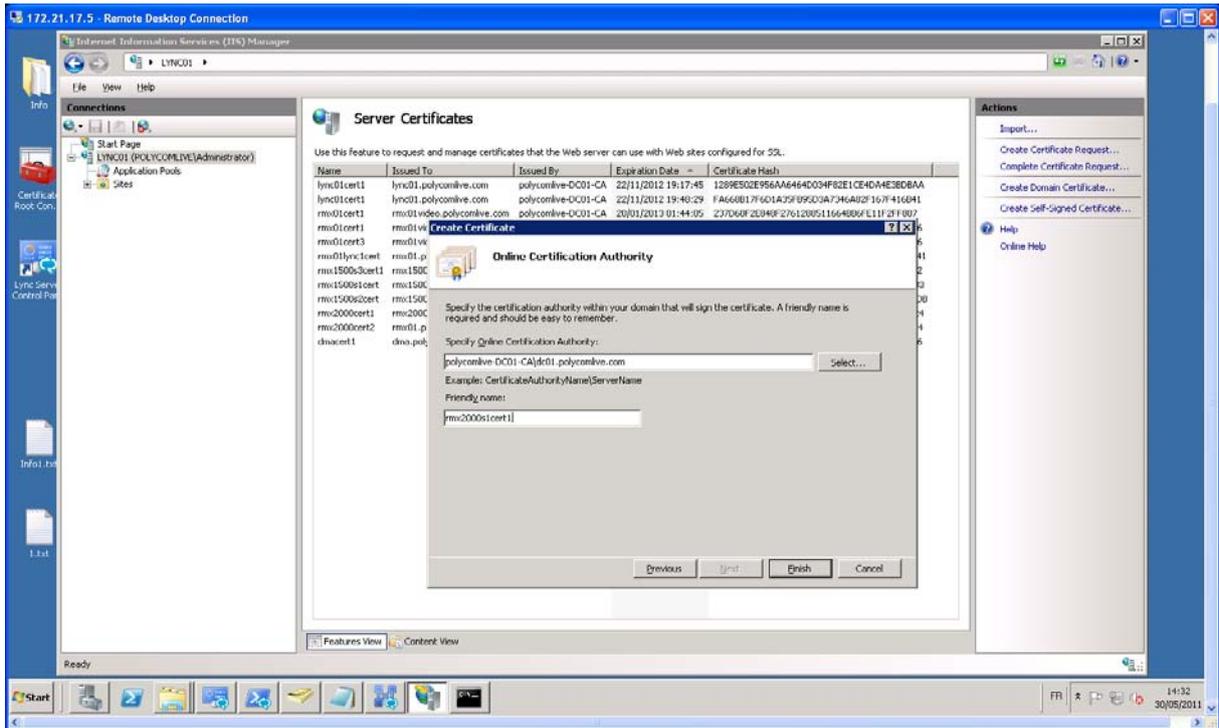
Right click in the blank area and select "Create Domain Certificates"

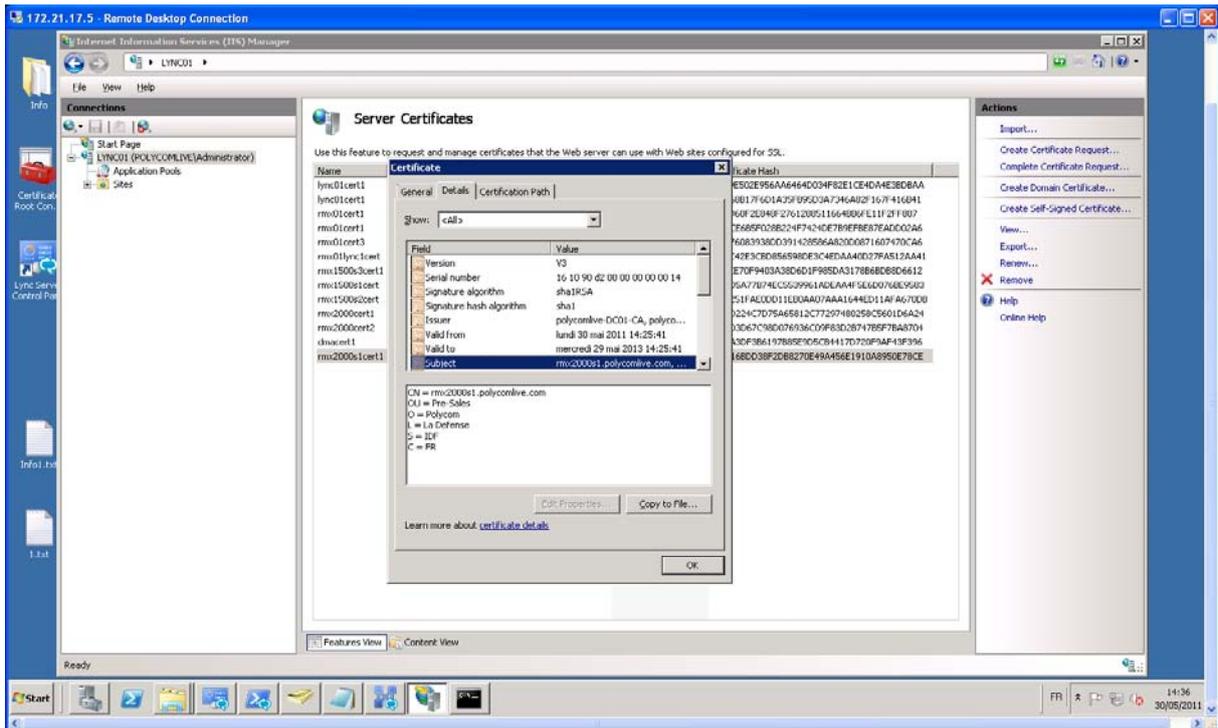
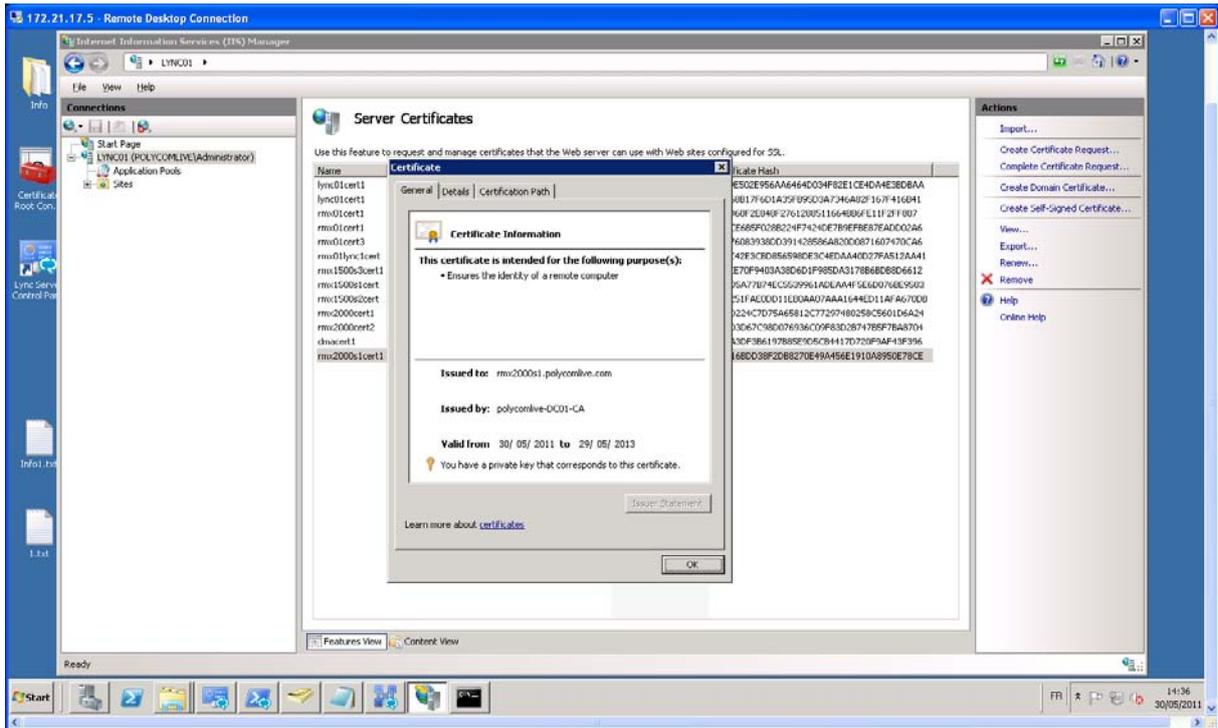


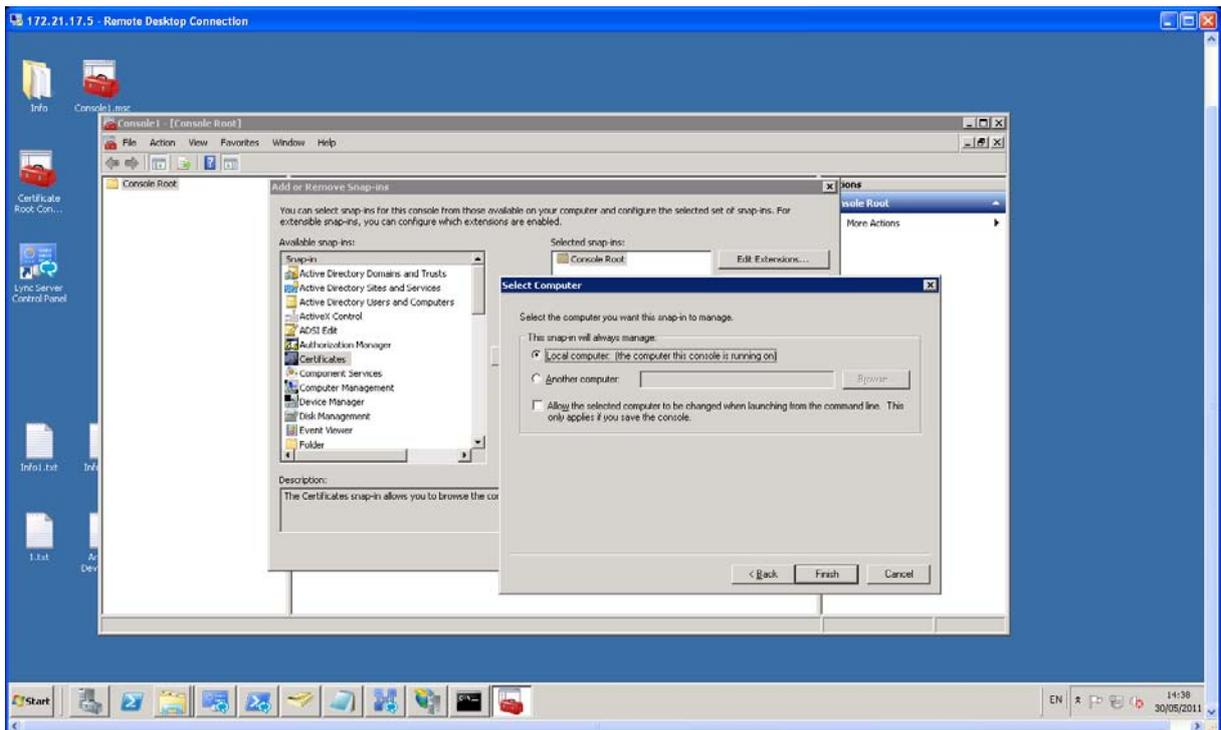
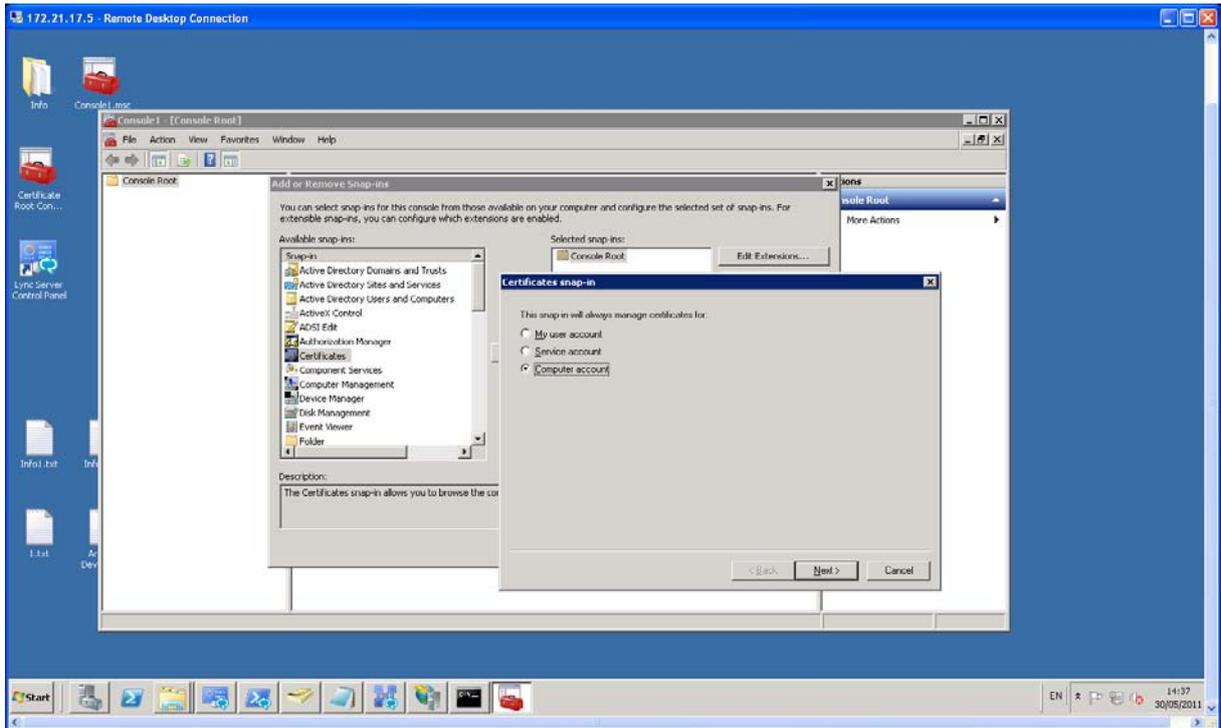
Create a Security Certificate for the Polycom RMX System

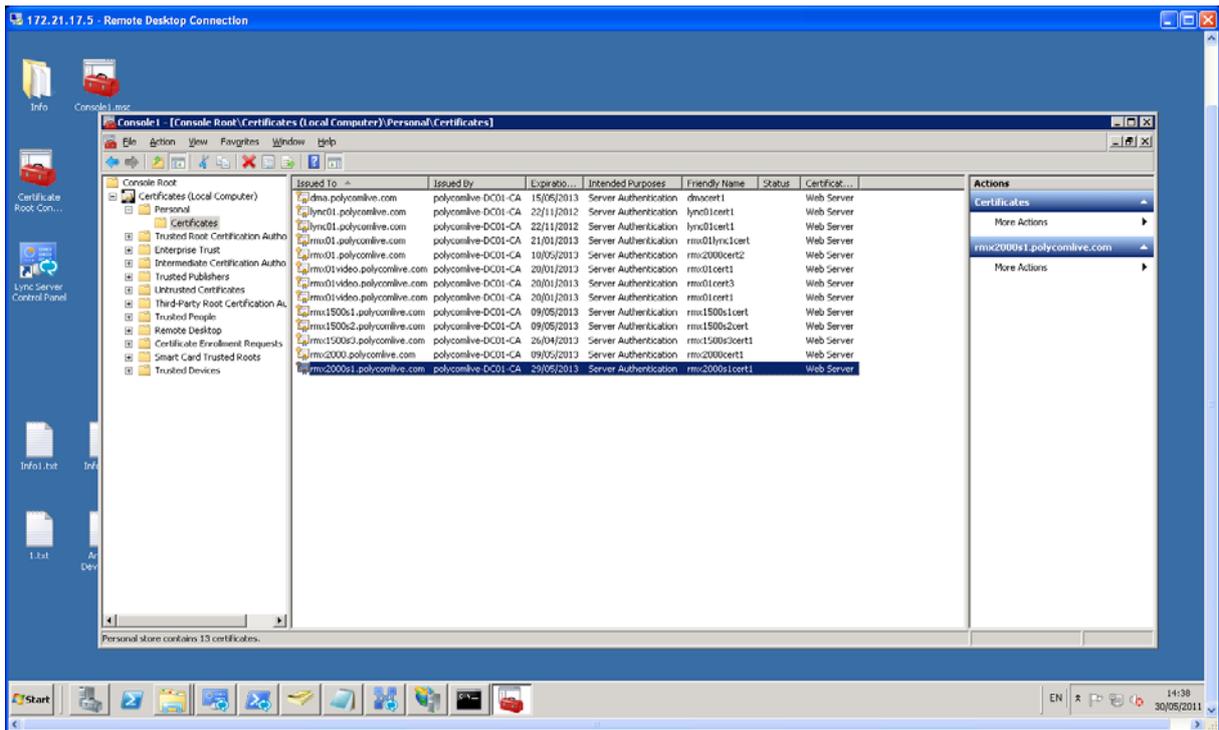
In common name, enter the FQDN of the RMX server that had been entered as a DNS record in DNS server.



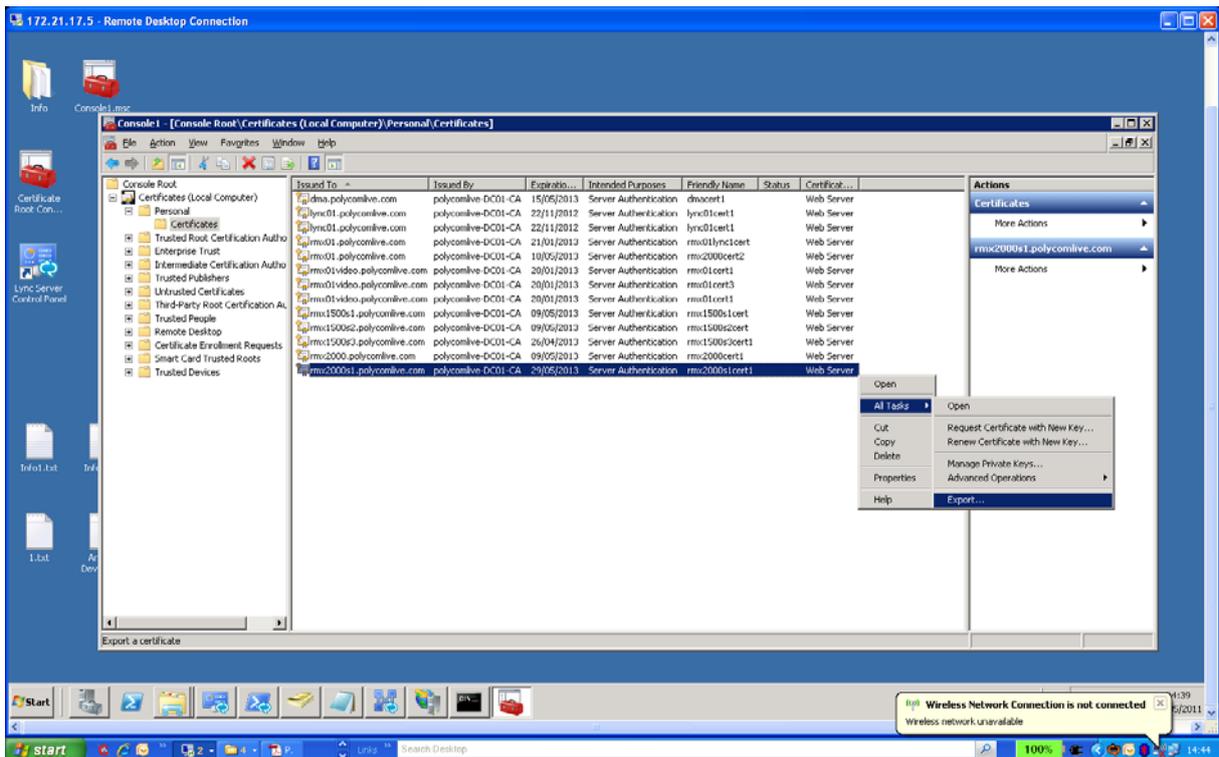


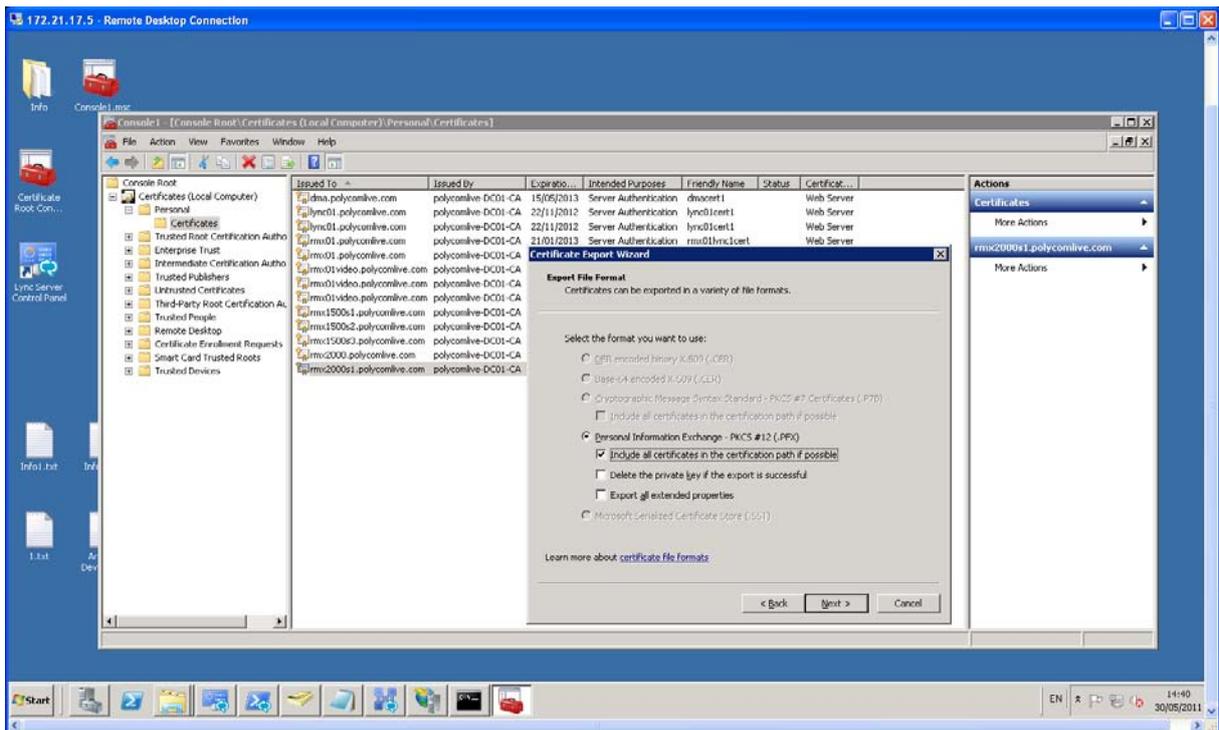
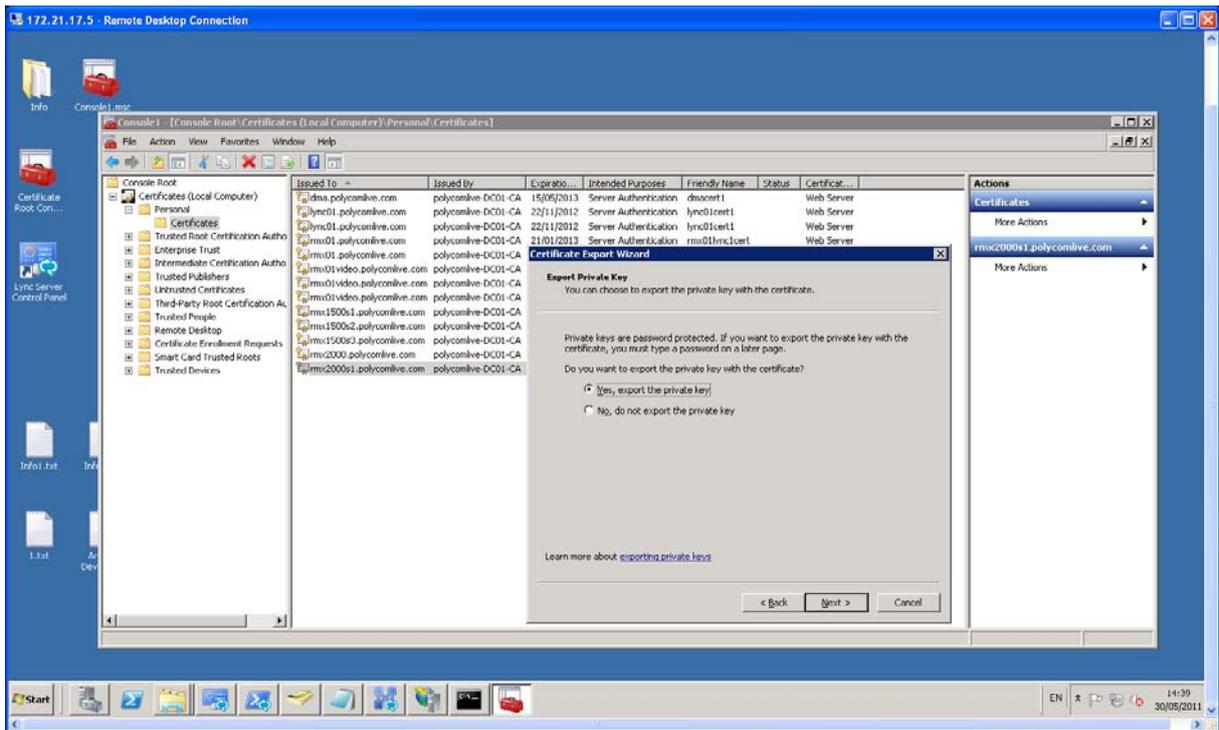




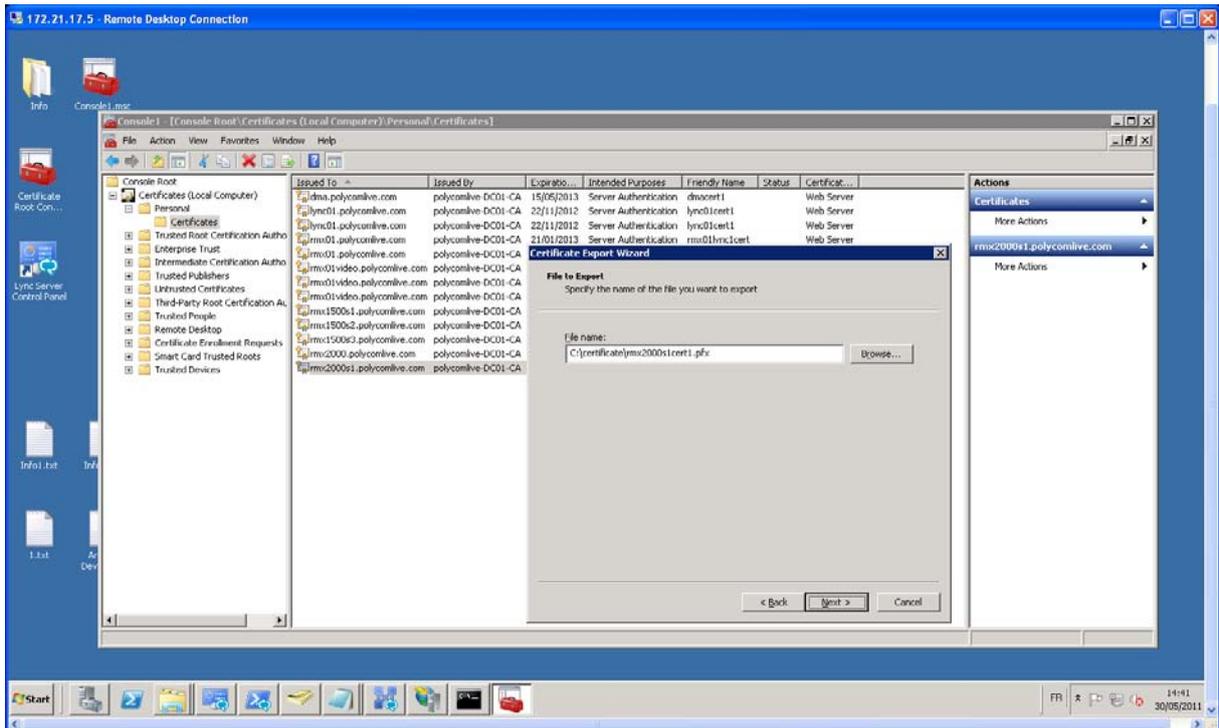
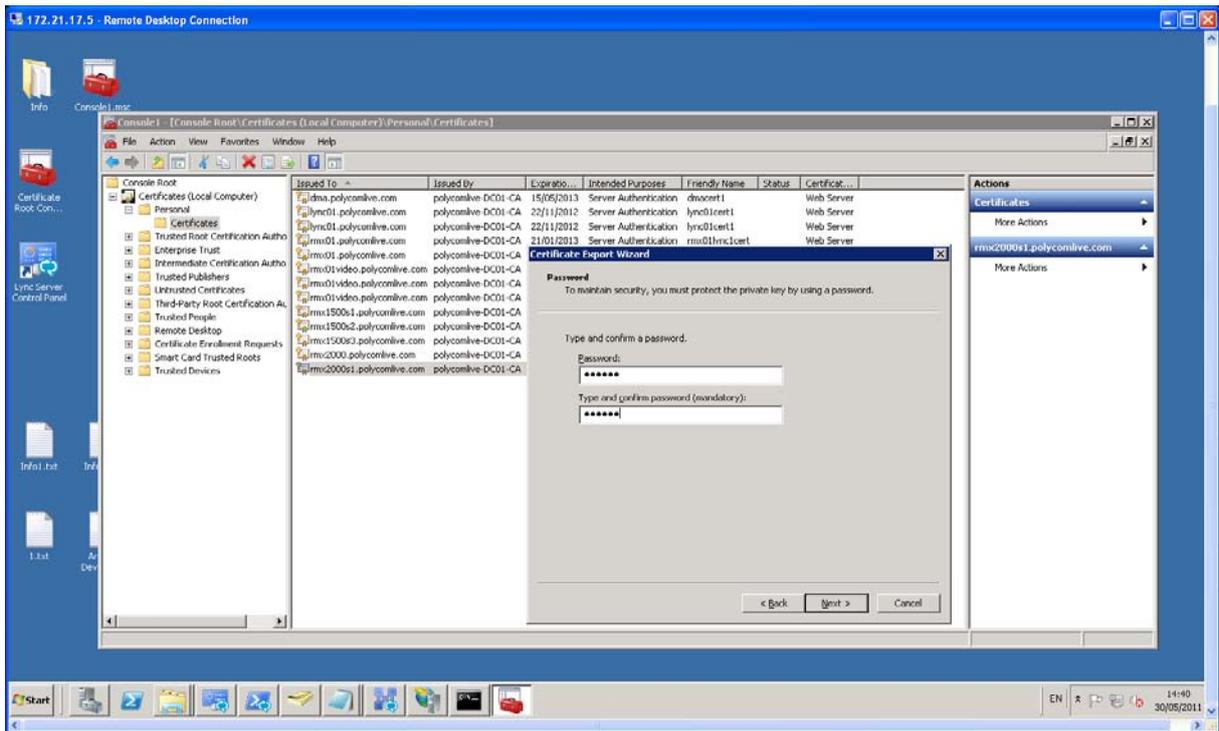


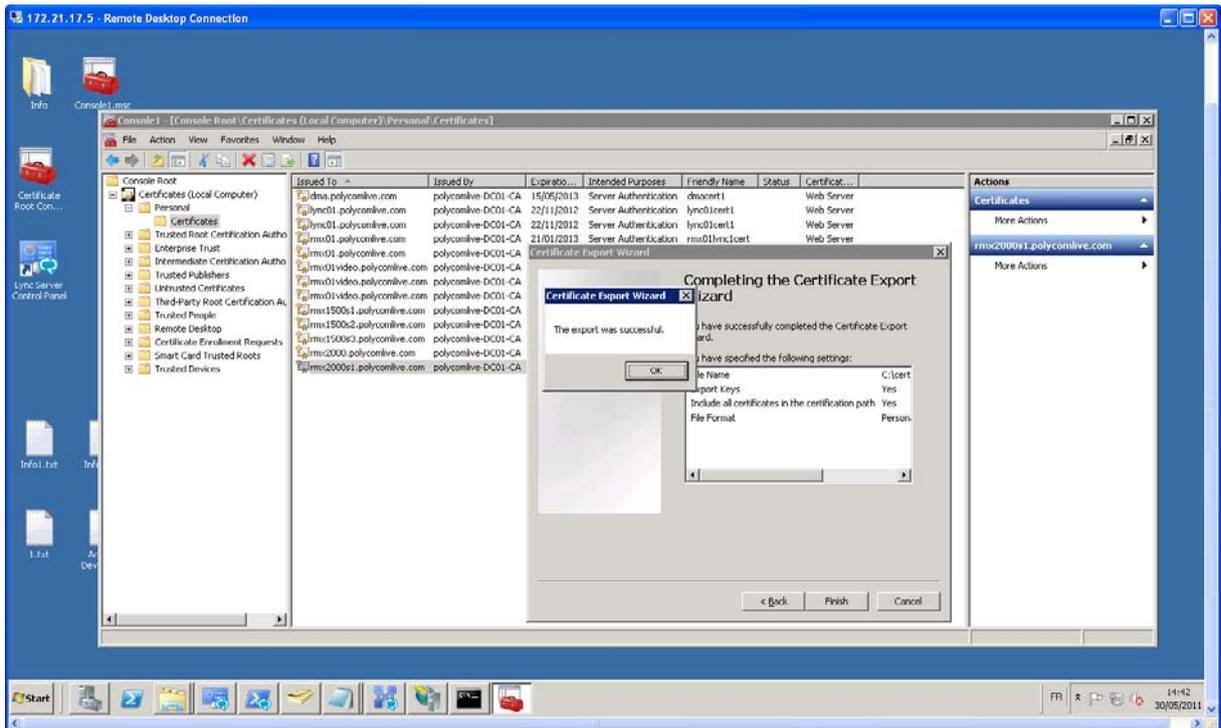
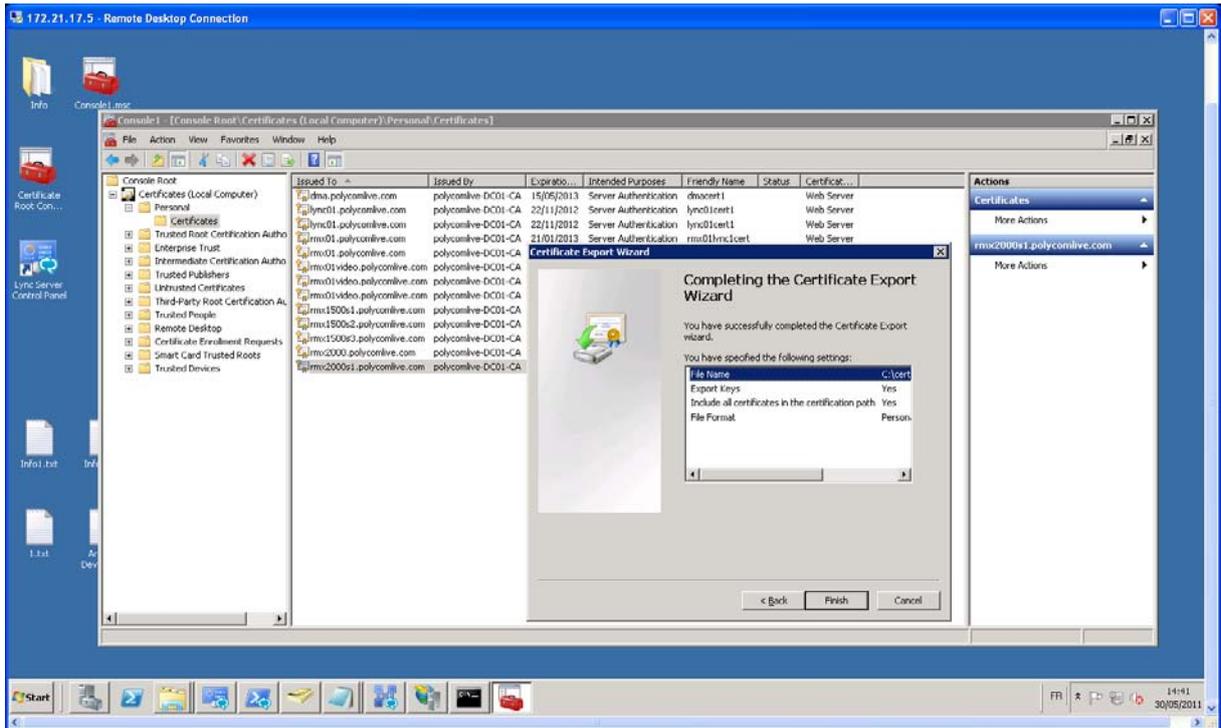
Then export this new created certificate, as shown below:





Enter the password for the pfx certificate, as shown below:





Set the SIP server settings in the RMX and import the certificate to RMX

First copy the new created PFX certificate from Lync server to a PC where you will connect to RMX and also create an empty **text file** called **certPassword.txt** in same folder where you had put the RMX certificate and then put the password you had entered for the certificate during its creation in the **certPassword.txt** file.

Then proceed with the following actions.

IP Network Type: **H323 & SIP**

SIP Server: **Microsoft**

In SIP Servers put the information as mentioned below:

Server FQDN: **lync01.polycomlive.com** (you will need to put the FQDN of your lync server)

Server Domain Name: **polycomlive.com** (you will need to put the domain name of the where your lync server is located)

Port: **5061**

Same for Outbound proxy server

IP Network Service Properties

- >> Networking
- > IP
- > Routers
- >> Conferencing
- > Gatekeeper
- > Ports
- > QoS
- > **SIP Servers**
- > Security
- > SIP Advanced

Network Service Name: IP Network Service

IP Network Type: H.323 & SIP

SIP Server: Specify

SIP Server Type: Microsoft

Refresh Registration every: 3600 seconds

Transport Type: TLS Create Certificate

Certificate Method: CSR Send Certificate

SIP Servers:

Parameter	Primary Server	Alter
Server IP Address or Name	lync01.polycomlive.com	
Server Domain Name	polycomlive.com	
Port	5061	

Outbound Proxy Servers:

Parameter	Primary Server
Server IP Address or Name	lync01.polycomlive.com
Port	5061

OK Cancel

Then upload the new created certificate as shown below by selecting the certificate Method as **PEM/PFX**:

The screenshot shows the 'IP Network Service Properties' dialog box. On the left is a navigation tree with 'SIP Servers' selected. The main area contains the following settings:

- Network Service Name: IP Network Service
- IP Network Type: H.323 & SIP
- SIP Server: Specify
- SIP Server Type: Microsoft
- Refresh Registration every: 3600 seconds
- Transport Type: TLS
- Certificate Method: PEM/PFX
- Send Certificate button (highlighted)

Below these settings are two tables for SIP Servers and Outbound Proxy Servers:

SIP Servers:

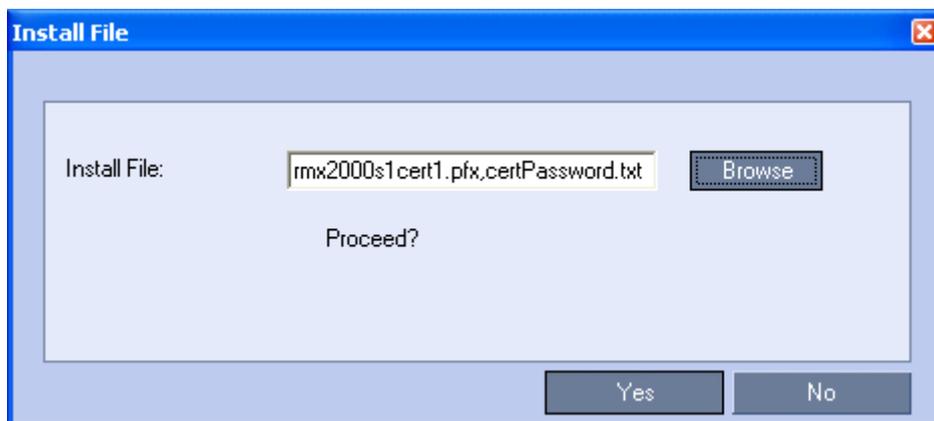
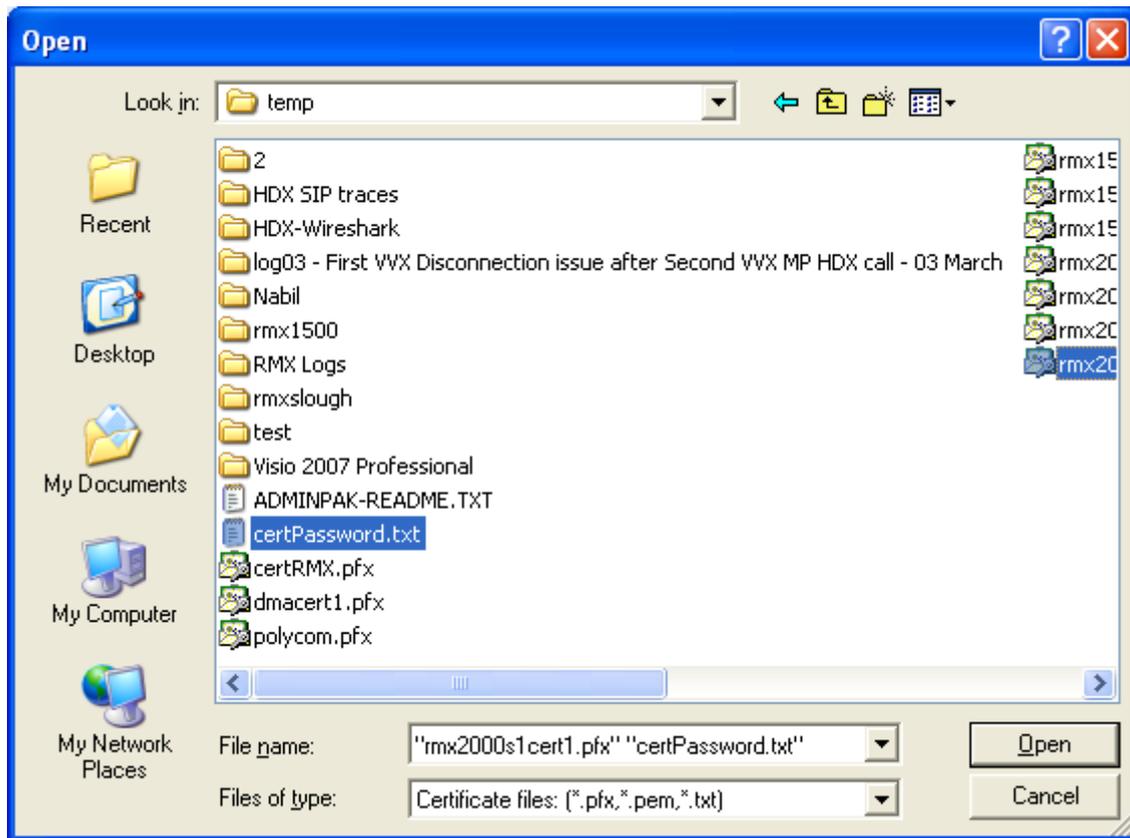
Parameter	Primary Server	Alter
Server IP Address or Name	lync01.polycomlive.com	
Server Domain Name	polycomlive.com	
Port	5061	

Outbound Proxy Servers:

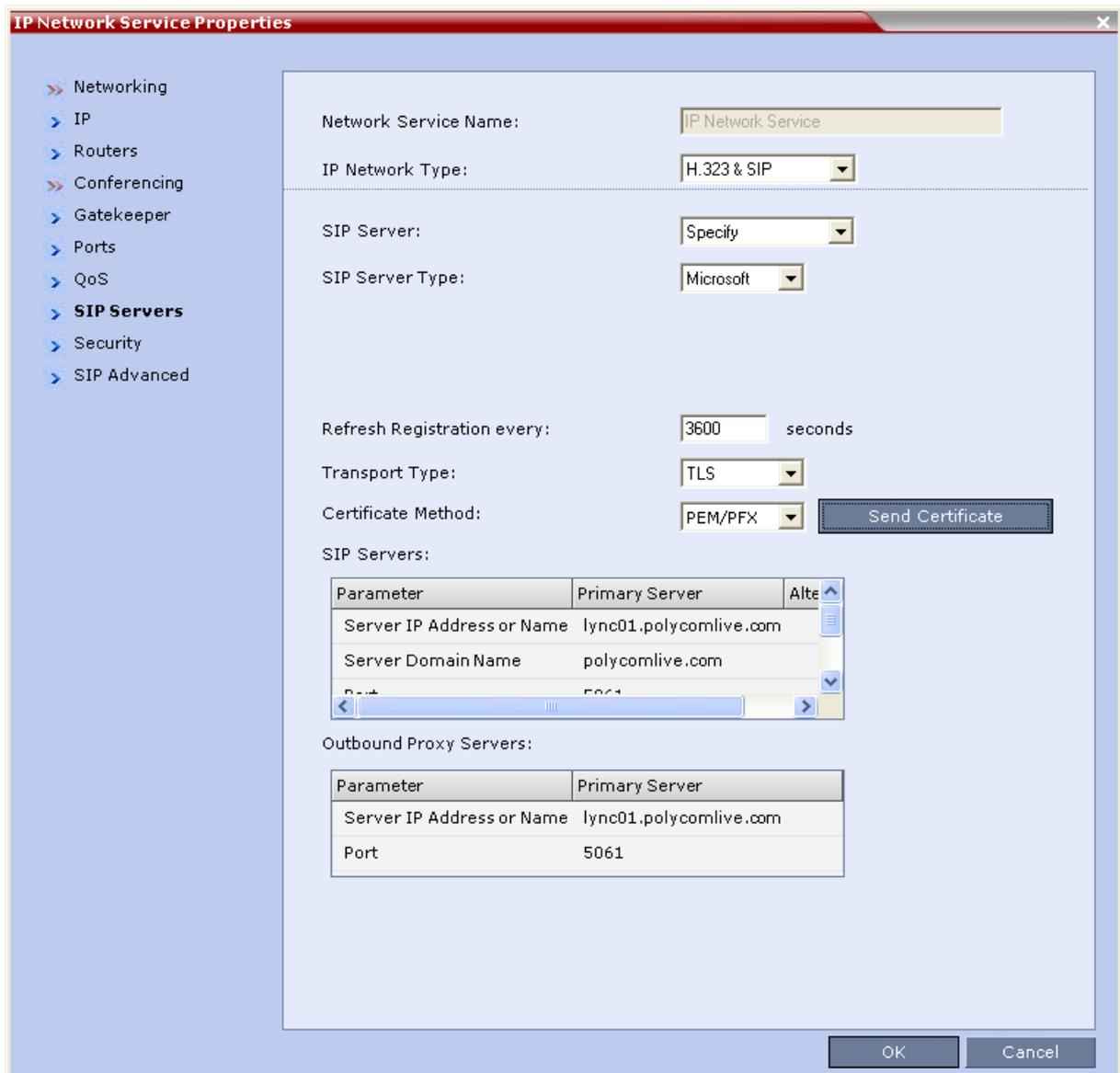
Parameter	Primary Server
Server IP Address or Name	lync01.polycomlive.com
Port	5061

At the bottom right are 'OK' and 'Cancel' buttons.

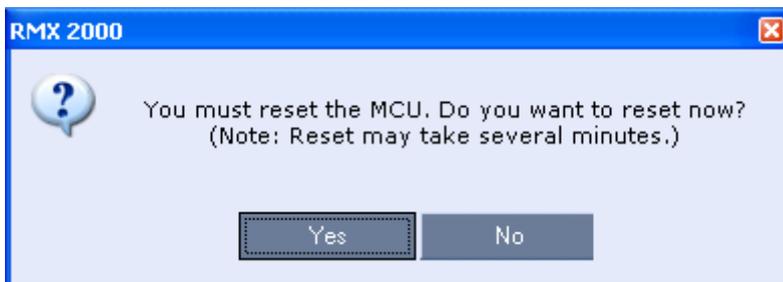
Then select both files the **certificate file** and the **certPassword text file** in same time by using the CTRL key and the mouse by clicking each time in the first and then on the second file.

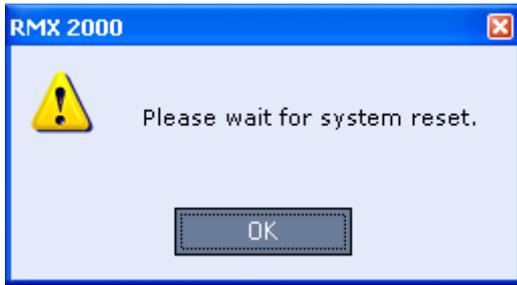


Then click on “Yes”.



Then RMX will ask you that it will reboot. Select "Yes".





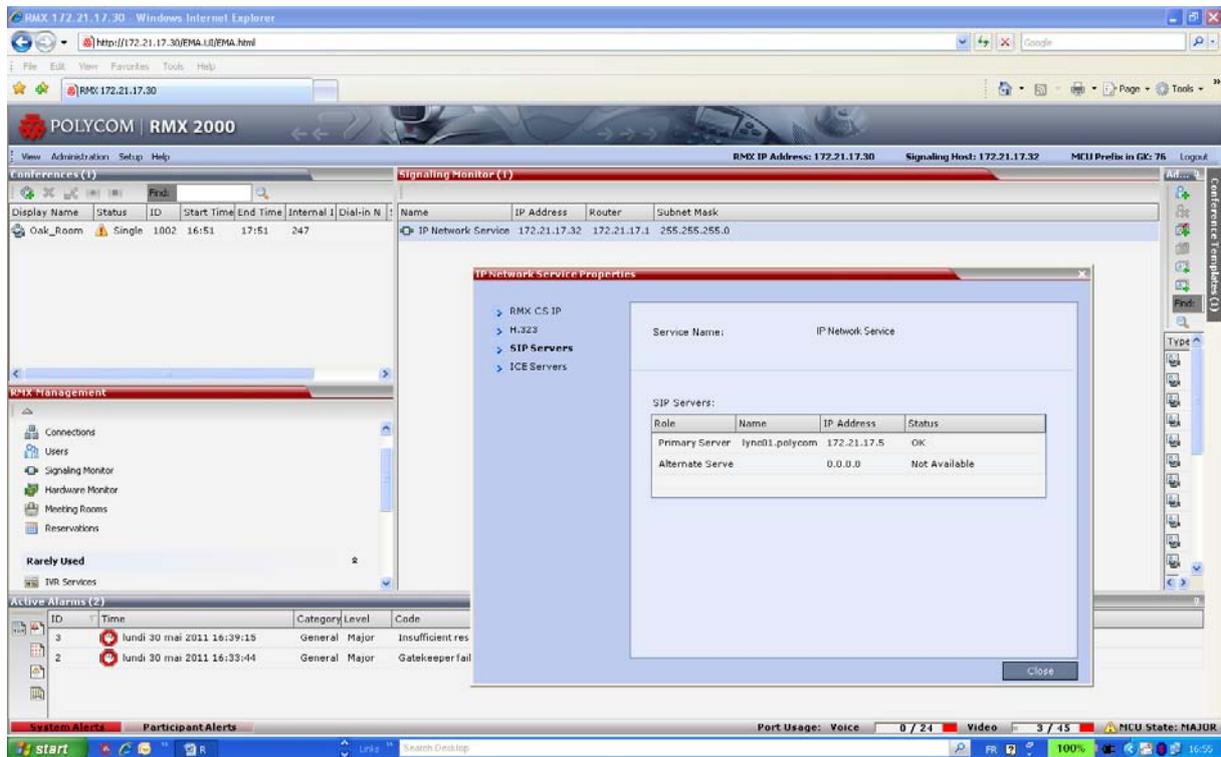
After the RMX reboot, you should not have any TLS error in the alarm monitor, as shown below:

The screenshot shows the RMX 2000 web interface in Internet Explorer. The main content area is empty. The "Active Alarms (2)" section at the bottom contains the following table:

ID	Time	Category	Level	Code	Process Name	Description
3	lundi 30 mai 2011 16:39:15	General	Major	Insufficient resources	Resource	Insufficient resources
2	lundi 30 mai 2011 16:33:44	General	Major	Gatekeeper failure	Gatekeeper	GK_Rejected_GRQ_Reason_Is_Resource_Unavailable, (to: 1d1)

At the bottom of the interface, there is a status bar showing "Port Usage: Voice 0 / 24 Video 0 / 45" and "MCU State: MAJOR".

Then, check in the Signaling Monitor, in SIP Server and you should see the IP address of Lync server with status as "OK".



Then go on a PC client and open Lync and enter for example the following SIP URI to call Meeting Room 1002 in RMX from Lync client:

1002@rmx2kvideo.polycomlive.com

RMX will answer and you will see the video out from RMX to Lync client as shown below.

